Turla APT actor refreshes KopiLuwak JavaScript backdoor for use in G20-themed attack

AUGUST 17, 2017 | DARIEN HUSS

Overview

Proofpoint researchers have observed a well-known Russian-speaking APT actor usually referred to as Turla using a new .NET/MSIL dropper for an existing backdoor called JSHolgi.uwak. The backdoor has been analyzed previously [1] and is a robust tool associated with this group, likely being used as an early stage reconnaissance tool.

In this case, the dropper is being delivered with a benign and possibly stolen decoy document inviting recipients to a G20 task force meeting on the "Digital Economy". The Digital Economy event is actually scheduled for October of this year in Hamburg, Germany. The dropper first appeared in mid-July, suggesting that the APT activity is potentially ongoing, with Turla actively targeting G20 participants and/or those with interest in the G20, including member nations, journalists, and policymakers. This blog provides details on the dropper and known information on the infection chain and current related Turla activity.

Actor Overview

Turla is a well-documented, long-operating APT group that is widely believed to be a Russian state-sponsored organization. Turla is perhaps most notoriously suspected as responsible for the breach of the United States Central Command in 2008 [1]. More recently Turla was accused of breaching RUAG, a Swiss technology company, in a public report published by GovCERT.ch [2]. Various other Turla frameworks, implants, and campaigns have been detailed extensively by our fellow security organizations and companies [3-10].

Delivery

The delivery of KopiLuwak in this instance is currently unknown as the MSIL dropper has only been observed by Proofpoint researchers on a public malware repository. Assuming this variant of KopiLuwak has been observed in the wild, there are a number of ways it may have been delivered including some of Turla's previous attack methods such as spear phishing or via a watering hole. Based on the theme of the decoy PDF, it is very possible that the intended targets are individuals or organizations that are or have interest in G20's Digital Economy Task Force. This could include diplomats, experts in the areas of interest related to the Digital Economy Task Force, or possibly even journalists.

Analysis

The earliest step in any possible attack(s) involving this variant of KopiLuwak of which Proofpoint researchers are currently aware begins with the MSIL dropper. The basic chain of events upon execution of the MSIL dropper include dropping and executing both a PDF decoy and a Javascript (JS) dropper. As explained in further detail below, the JS dropper ultimately installs a JS decryptor onto an infected machine that will then finally decrypt and execute the actual KopiLuwak backdoor in memory only (Fig. 1).

Figure 1: Diagram showing execution beginning with the MSIL dropper

As Proofpoint has not yet observed this attack in the wild it is likely that there is an additional component that leads to the execution of the MSIL dropper. This may include a malicious document, compressed package attached to an e-mail, or perhaps it could be delivered via a watering hole attack.

The KopiLuwak MSIL dropper is straightforward and contains absolutely no obfuscation or anti-analysis. Internally the MSIL dropper is called Runer.exe and also contains a PDB string "z:\LocalDisc_D\MyProjects\Runer\Runer\obj\Release\Runer.pdb". The Stage1 JS and PDF decoy are both stored in plaintext in the dropper and are written to %APPDATA% then executed (Fig. 2).

Figure 2: MSIL dropper writing both the Stage1 JS and decoy PDF then executing both

Both of the dropped files have hardcoded names: the JS is named Scr.js while the PDF is named Save the Date G20 Digital Economy Taskforce 23 24 October.pdf. The decoy in this case is an invitation to save the date for a meeting of the G20's Digital Economy Taskforce (Fig. 3) in Hamburg, Germany.

Federal Ministry for Economic Affairs and Energy

G20 GERMANY 2017

Berlin, 22 June 2017

Save the Date

Task Force "Digital Economy"

23-24 October in Hamburg

Dear Colleagues,

I hope that everyone has been well since we last met in April. By means of this letter I would like to ask you to "Save the Date" as we are planning another G20 Task Force "Digital Economy" meeting for 23-24 October 2017 in Hamburg.

In April, our Ministers endorsed the first ever G20 Digital Economy Ministerial Declaration. Now it is time to start putting it into action as part of the Declaration, the "ROADMAP for Digitalisation: Policies for a Digital Future" outlined eleven important areas that require our further attention. The meeting in October will allow us to implement some of these actions and help set the course for future work under the Argentinian Presidency.

Figure 3: PDF decoy with a "Save the Date" invitation to a G20 Digital Economy Taskforce meeting

As far as we are aware, this document is not publicly available and so may indicate that an entity with access to this document has already been compromised. Alternatively, the document may have been legitimately obtained from a recipient.

Proofpoint researchers ascertain with medium confidence that the document is legitimate and not fabricated. One piece of evidence suggesting that the document could be authentic is that in the document's exif metadata, the creator tool is listed as 'BE D4 113.1' (Fig. 4) which matches another PDF document that appears to have been scanned and is hosted on the Bundesministerium für Wirtschaft and Energie website (Fig. 5).

Figure 4: Exif metadata from the decoy document

Figure 5: Exif metadata from the PDF hosted on bmwi[.]de

BMWi, which translates to Federal Ministry for Economic Affairs and Energy, is the organization from which the decoy document supposedly originated. Both documents were also supposedly created on a KONICA MINOLTA bizhub C284e according to their exif metadata.

Scr.js Analysis

Scr.js is essentially a dropper for the actual backdoor in addition to running all the necessary commands to fingerprint the infected system and set up persistence. Scr.js first creates a scheduled task named PolicyConverter for persistence. This scheduled task should execute shortly after being created and is then scheduled to run every 10 minutes. The scheduled task is executed with the following parameters: "appidpolicyconverter.js FileType/XML gerV4jlJG3xlq7z5fRG". Similar to the older KopiLuwak variant, the second parameter is used as an RC4 key to decrypt the encrypted JS backdoor code contained in appidpolicyconverter.js.

Next, Scr.js provides a large base64 blob containing the JS backdoor decryptor and saves it to the following location: "C:\Users[executing user]\AppData\Roaming\Microsoft\Proto\appidpolicyconverter.js".

Lastly, Scr.js executes various commands to fingerprint details about the infected system. In the older variant of KopiLuwak, these commands were executed directly from the backdoor JS. Now, however, they have been moved to the dropper. Despite moving the machine fingerprinting code to the dropper, all of the commands are the same as in the older sample (and executed in the same order) except for the following three additions:

• dir "[programfiles]%\Kaspersky Lab"
• dir "[programfiles(x86)%\Kaspersky Lab"
• tracert www.google.com

Interestingly the only anti-virus company that is specifically fingerprinted is Kaspersky, which was possibly added as a result of their public analysis of this backdoor. The output from the commands are saved to the following location: "[appdata]%\Microsoft\Proto\~~.tmp"

appidpolicyconverter.js Analysis

The appidpolicyconverter.js script contains a large string that is first base64-decoded then RC4-decrypted using the supplied parameter as a key ("gerV4jlJG3xlq7z5fRG") from the executed task. Once the KopiLuwak backdoor code is successfully decrypted, it is then executed with eval().

The decrypted code functions similarly to the original KopiLuwak discussed by Kaspersky with some slight changes. The backdoor still communicates with what appear to be two compromised, legitimate websites using HTTP POST requests (Fig. 6).

Figure 6: Hardcoded legitimate, compromised command and control servers

Differing from the older sample, the HTTP User-Agent is now hardcoded and no longer contains a component unique to each infected machine.

Each HTTP POST request sent to the command and control (C&C) will contain information in its client body. The planted content is first preceded with a hardcoded key "Pn(14hhaV_kB0hlY3". Next, the key is followed by a separator string "nddd". Next, the hardcoded key "Pn(14hhaV_kB0hlY3" is used to encode the infected system's OS installation date (Fig. 7).

Figure 7: Retrieving the OS installation date

If any additional information is being sent to the C&C it will then be appended after the encoded installation date. Finally, the data is encrypted with RC4 using a hardcoded key: "01e8cbd228dff18f4698f85df68e2879431f" and then queried (Fig. 8).

Figure 8: HTTP POST to KopiLuwak C2

Responses from the command and control are also encrypted using RC4 and the same key. After responses from the C&C are decrypted, they are compared to a list of supported commands. This newer variant of KopiLuwak has several different supported keywords, including one additional command, giving a total of five commands versus the old variant's four (Table 1).

Command	Description
	Send the content infected system's fingerprint info saved in ~~.tmp and sent
–cpixl	Exfiltrate content from provided filename (from C1) to C2. Max exfiltration file size is in 104857600 bytes (1MB)
–kill	Two options for this command: • execute provided JS using eval; send contents of ~~.tmp to C2, then exfiltration file size is in 104857600 bytes (1MB)
–wait	End the script. The scheduled task would execute the backdoor again in ~10 minutes
–dwld	Saves the provided content with provided extension to [appdata]%\Microsoft\Proto\[filename]; if successful sends success message to C2

Table 1: KopiLuwak supported commands and descriptions

The newer variant of KopiLuwak is now capable of exfiltrating files to the C&C as well as downloading files and saving them to the infected machine. Although these capabilities could have been accomplished in the previous variant by executing arbitrary commands, they are now implemented with their own dedicated commands. Despite the added capabilities, we still agree with Kaspersky that this backdoor is likely used as an initial reconnaissance tool and would probably be used as a staging point to deploy one of Turla's more fully-featured implants. We also believe this backdoor will continue to be used in the future as is suggested by the continued development of the backdoor itself as well as the new delivery mechanisms.

Conclusion

Because the samples were obtained from a public malware repository and we have not yet observed them in the wild, the full scope and impact of the attack (or, possibly, a pending attack) cannot be fully assessed. However, for PCs running the .NET framework (which includes most modern Windows operating systems), the potential impact is high:

• The JavaScript dropper profiles the victim's system, establishes persistence, and installs the KopiLuwak backdoor.
• KopiLuwak is a robust tool capable of exfiltrating data, downloading additional payloads, and executing arbitrary commands provided by the actor(s)

The high profile of potentially targeted individuals associated with the G20 and early reconnaissance nature of the tools involved bear further watching. We have notified CERT-Bund of this activity.

We will continue to track the activities associated both with this actor and these new tools and update this blog as details emerge.

References

[1] https://en.wikipedia.org/wiki/2008_cyberattack_on_United_States
[2] https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case
[3] https://securelist.com/the-epic-turla-operation/65545/
[4] https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
[5] https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf
[6] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
[7] https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
[8] https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/
[9] https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
[10] http://www.gdatasoftware.com/blog/2015/01/23926-analysis-of-project-cobra
[11] https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/

Indicators of Compromise (IOCs)

KopiLuwak MSIL Dropper

7461a670d306ec5342d2336542dc1d268572b0ed11c1347677bde8dc5239ad5b

KopiLuwak JS Dropper "Scr.js"

1c76a68a670a69b4fee29ca0ffea6be849c4a30d3ad4a661da3b4eb82ae19

KopiLuwak JavaScript Decryptor "appidpolicyconverter.js"

9686c9f2b1efbe87abc0ff9e2c7597844734485dc6b2e802aeaccbb0edc27fad

Benign PDF Decoy "Save the Date G20 Digital Economy Taskforce 23 24 October.pdf"

c92b7da3ecccf7a79d27d00e4d6e9de4c99a69dd4c8dc45e61ba5e0aca25dd1b

KopiLuwak C&C

hxxp://www[.hunival].de/wp-content/plugins/wordpress-connect/includes/class-wp-org.php
hxxp://faizor-rent[.]com/fm/wp-content/plugins/wordpress-seo/vendor/ircmaxell/password-compat/lib/loader.php

ET and ETPRO Suricata/Snort Coverage

2827574 ETPRO TROJAN Turla JSMsil.uwak CnC Beacon M1
2827575 ETPRO TROJAN Turla JSMsil.uwak CnC Beacon M2

About
Overview
Why Proofpoint
Careers
Leadership Team
News Center
Investors Center

Threat Center
Latest Threat Report
Human Factor Report
Threat Glossary
Threat Blog
Daily Ruleset

Products
Email Protection
Advanced Threat Protection
Security Awareness Training
Cloud App Security
Information Protection
Digital Risk Protection
Product Bundles
Nexus Platform

Resources
Whitepapers
Webinars
Datasheets
Events
Customer Stories
Blog
Free Trial

Connect
📞 +1 408-517-4710
Contact Us
Office Locations
Request a Demo

Support
Support Login
Support Services
IP Address Blocked?