New Andariel Reconnaissance Tactics Uncovered

trendmicro.com/en_us/research/18/g/new-andariel-reconnaissance-tactics-hint-at-next-targets.html

July 16, 2018

APT & Targeted Attacks

Some groups go to great lengths to investigate their targets' systems. A recent example is the Andariel Group, a branch of the Lazarus Group. We tracked new scouting techniques coming from Andariel, used mainly against South Korean targets.

By: Joseph C Chen July 16, 2018 Read time: (words)

Updated June 18, 2018, 10:05 AM to add new IoC information from IssueMakersLab's July investigation. We updated it again at 4:30 PM to add a link to IssueMakersLab's website and to add new IoC information. This research is done in cooperation with IssueMakersLab of South Korea.

Reconnaissance plays a vital role in criminal operations, and some groups go to great lengths to investigate their targets' systems. A recent example is the Andariel Group, a known branch of the notorious Lazarus Group. Last month we tracked new scouting techniques coming from Andariel, which were used mainly against South Korean targets.

Andariel has been quite active these past few months. According to South Korean security researchers IssueMakersLab, the group used an ActiveX zero-day exploit for watering hole attacks on South Korean websites last May—they called this “Operation GoldenAxe”. But more recently on June 21, we noticed that Andariel injected their script into four other compromised South Korean websites for reconnaissance purposes.

We found that the code of the new injected script is similar to the sample Andariel previously used in May. However, the new script was trying to collect different ActiveX object information and targeted objects that it wasn’t attacking before.

In the earlier case, the group collected targeted ActiveX objects on users’ Internet Explorer browser before they used the zero-day exploit. This was possibly part of their reconnaissance strategy, to find the right targets for their exploit. Based on this, we believe it's likely that the new targeted ActiveX objects we found could be their next targets for a watering hole exploit attack. To help prevent any damage, we decided to publish our findings before the group deploys the attack.

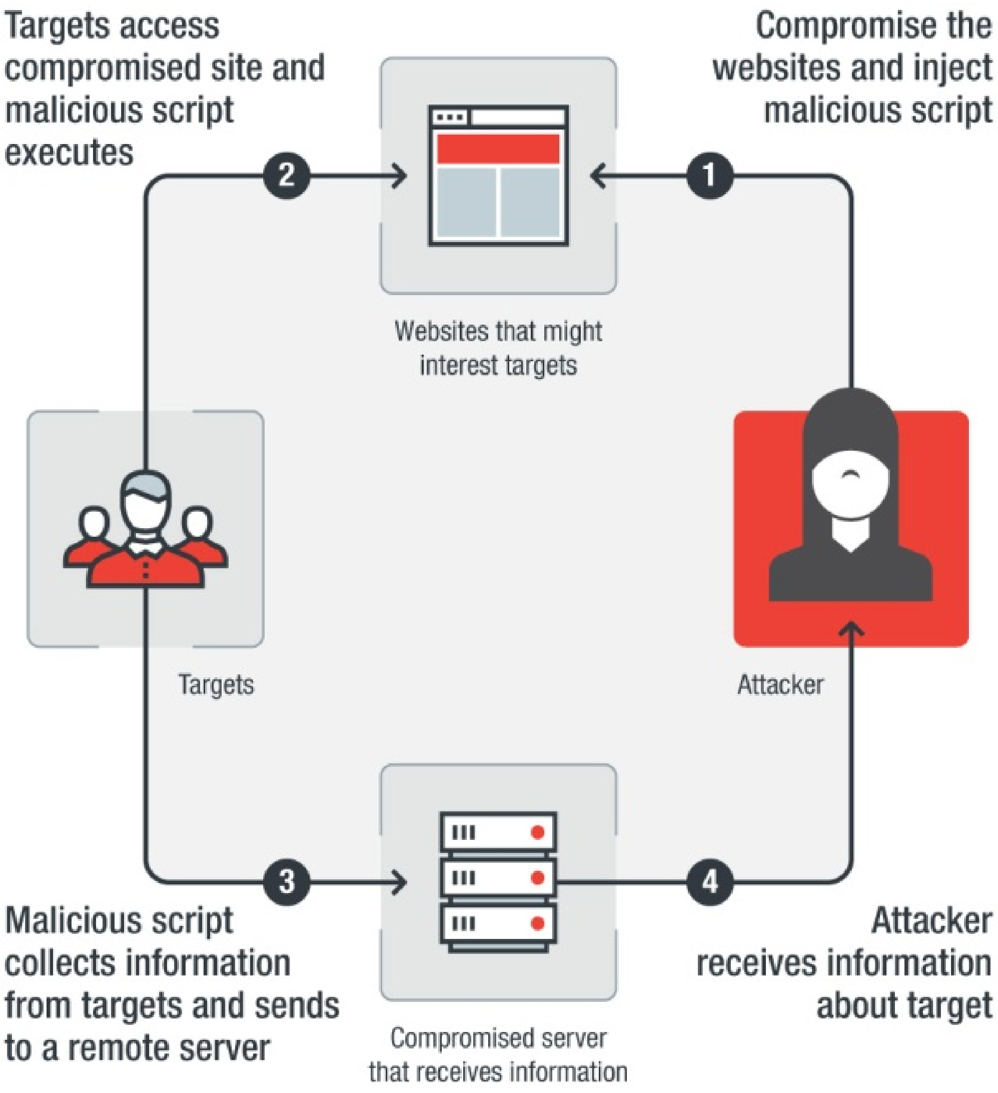

Targets access compromised site and malicious script executes
Compromise the websites and inject malicious script
2
1
Websites that might interest targets
Targets
Attacker
3
4
Malicious script collects information from targets and sends to a remote server
Compromised server that receives information
Attacker receives information about target

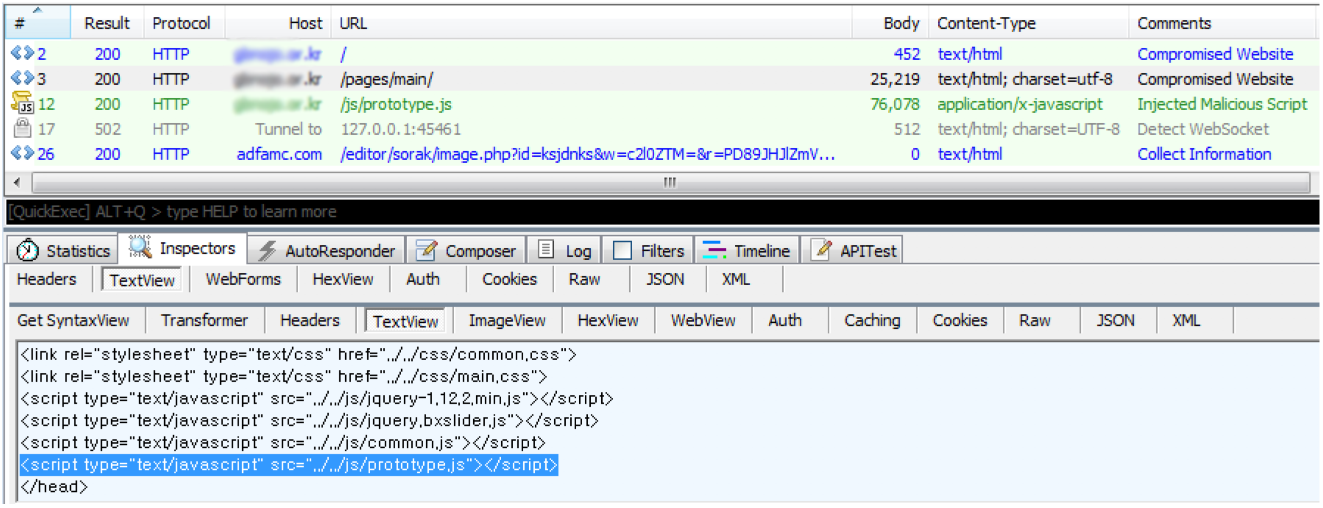
Figure 1. Watering hole reconnaissance flow

Analysis of the Andariel techniques

On June 21, we found that the website of a Korean non-profit organization was compromised with an injected script that collected visitors' information. We also found the same script on three South Korean local government labor union websites. This reconnaissance lasted until 27 June. We already notified the websites about the compromise.

We believe that the injected script came from the Andariel group since the code has similar obfuscation and structure to the sample we previously found from them. The script was used to collect information from visitors' browser: browser type, system language, Flash Player version, Silverlight version, and multiple ActiveX objects.

The original script is from the PluginDetect Library, and it was also used by exploit kits to verify victims before an attack. The verification process included sending collected information to another compromised website that hosted their PHP program and was designed to receive the information.



#	Result	Protocol	Host	URL	Body	Content-Type	Comments
2	200	HTTP	[redacted]	/	452	text/html	Compromised Website
3	200	HTTP	[redacted]	/pages/main/	25,219	text/html; charset=utf-8	Compromised Website
12	200	HTTP	[redacted]	/js/prototype.js	76,078	application/x-javascript	Injected Malicious Script
17	502	HTTP	Tunnel to	127.0.0.1:45461	512	text/html; charset=UTF-8	Detect WebSocket
26	200	HTTP	adfamc.com	/editor/sorak/image.php?id=ksjdnks&w=c2l0ZTM=&r=PD89JHJlZmV...	0	text/html	Collect Information

```
<link rel="stylesheet" type="text/css" href="../../css/common,css">
<link rel="stylesheet" type="text/css" href="../../css/main,css">
<script type="text/javascript" src="../../js/jquery-1,12,2,min,js"></script>
<script type="text/javascript" src="../../js/jquery,bxslider,js"></script>
<script type="text/javascript" src="../../js/common,js"></script>
<script type="text/javascript" src="../../js/prototype,js"></script>
</head>
```

Figure 2. Compromised website injected with malicious script that collects information

Our colleagues from the IssueMakersLab team shared insights and information about the Andariel group, including that they attacked ActiveX vulnerabilities as far back as 2007. The team monitoring Andariel found that the cybercriminal group injected a malicious script on a South Korean think tank website for reconnaissance in January 2017 and then switched to inject an ActiveX zero-day exploit in mid-April. IssueMakersLab also listed the ActiveX objects that the Andariel group attacked.

During analysis, we noticed that the new injected script was trying to detect two additional ActiveX objects that were not on the previous list. One is “DSDOWNCTRL.DSDownCtrlCtrl.1”, which is related to a DRM (Digital Rights Management) software from a South Korean Document Protection Security vendor. Another is “WSACTIVEBRIDGEAX.WSActiveBridgeAXCtrl.1”, which is related to a South Korea-based voice conversion software company. Many local governments and public institutions use these software.

We made a table to compare the information that the script samples collected in the previous case and this more recent case.

	Collected Information from Old Script Sample (May 2018)		**Collected Information from New Script Sample (June 2018)**
Parameter	**Meaning**	**Parameter**	**Meaning**

w	Website name	w	Website name
r	<?=$referer?> value	r	<?=$referer?> value
o	OS version	o	OS version
lv	HTTP Accept-Language	lv	HTTP Accept-Language
bt	Browser Information	bt	Browser Information
bv	Browser Information	bv	Browser Information
bdv	Browser Information	bdv	Browser Information
fv	Flash Version	fv	Flash Version
silv	Silverlight Version	silv	Silverlight Version
ez	EasyPayPlugin ActiveX Availability	ez	EasyPayPlugin ActiveX Availability
ac	ACUBEFILECTRL ActiveX Availability*	-	-
-	-	mg	MagicLoaderX ActiveX Availability
-	-	nv	NVersionMan ActiveX Availability
si	SIClientAccess ActiveX Availability	si	SIClientAccess ActiveX Availability
du	DUZONERPSSO ActiveX Availability	du	DUZONERPSSO ActiveX Availability
iw	INIWALLET61 ActiveX Availability	-	-
-	-	admctrl ActiveX Availability	
-	-	dw	DSDownCtril ActiveX Availability**
-	-	ab	WSActiveBridgeAX ActiveX Availability***
-	-	ve	Voice Conversion Software “*WSActiveBridge”* WebSocket Availability****

* detection of the previous ActiveX zero-day object

** detection of the ActiveX object related to DRM software (one of the new targets)

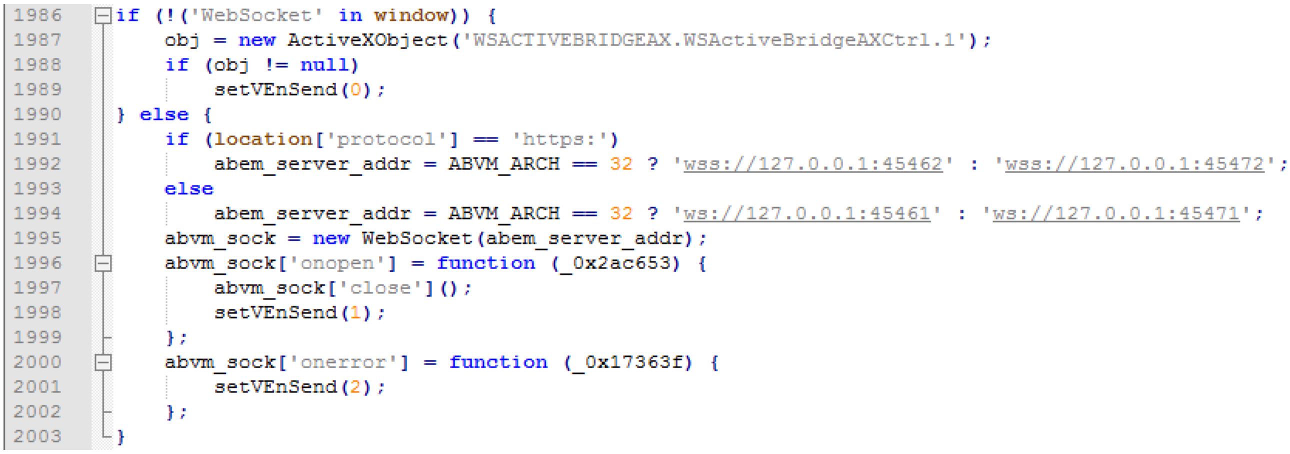
*** detection of the ActiveX object related to voice conversion software (one of the new targets)

**** detection of the WebSocket related to voice conversion software (one of the new targets)

Table 1. Comparison of the information collected by the previous and new script

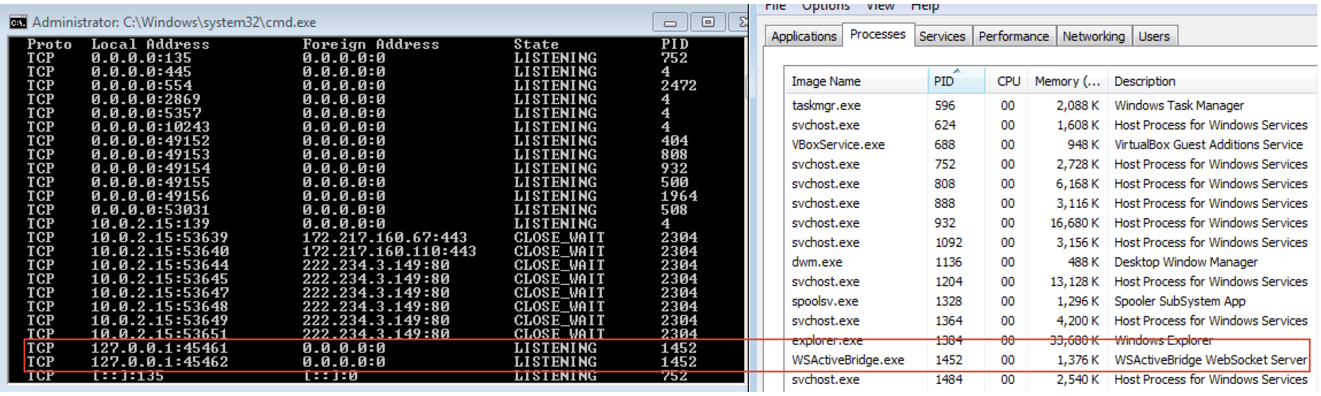
Besides the ActiveX objects, we noticed that the script added new code to connect *websocket* to *localhost*. The voice conversion software has *websocket* service listening on the local host so the injected script can detect the software by checking if they can establish a connection to ports 45461 and 45462, which the software uses.

In addition, the verification process in the older script is different from the ActiveX detection, which was only for the Internet Explorer browser. In the script found in June, the websocket verification could also be performed on other browsers like Chrome and Firefox. This shows that the attacker has expanded his target base, and is interested in the software itself and not just their ActiveX objects. Based on this change, we can expect them to start using attack vectors other than ActiveX.



```
if (!('WebSocket' in window)) {
    obj = new ActiveXObject('WSACTIVEBRIDGEAX.WSActiveBridgeAXCtrl.1');
    if (obj != null)
        setVEnSend(0);
} else {
    if (location['protocol'] == 'https:')
        abem_server_addr = ABVM_ARCH == 32 ? 'wss://127.0.0.1:45462' : 'wss://127.0.0.1:45472';
    else
        abem_server_addr = ABVM_ARCH == 32 ? 'ws://127.0.0.1:45461' : 'ws://127.0.0.1:45471';
    abvm_sock = new WebSocket(abem_server_addr);
    abvm_sock['onopen'] = function (_0x2ac653) {
        abvm_sock['close']();
        setVEnSend(1);
    };
    abvm_sock['onerror'] = function (_0x17363f) {
        setVEnSend(2);
    };
}
```

Figure 3. Script (Deobfuscated) for detecting the voice conversion software ActiveX object and local websocket availability



```
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       752
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING       2472
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       404
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       808
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       932
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       1964
  TCP    0.0.0.0:53031          0.0.0.0:0              LISTENING       508
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    10.0.2.15:53639        172.217.160.67:443     CLOSE_WAIT      2304
  TCP    10.0.2.15:53640        172.217.160.110:443    CLOSE_WAIT      2304
  TCP    10.0.2.15:53644        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    10.0.2.15:53645        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    10.0.2.15:53647        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    10.0.2.15:53648        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    10.0.2.15:53649        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    10.0.2.15:53651        222.234.3.149:80       CLOSE_WAIT      2304
  TCP    127.0.0.1:45461        0.0.0.0:0              LISTENING       1452
  TCP    127.0.0.1:45462        0.0.0.0:0              LISTENING       1452
  TCP    [::]:135               [::]:0                 LISTENING       752
```

Image Name	PID	CPU	Memory (...	Description
taskmgr.exe	596	00	2,088 K	Windows Task Manager
svchost.exe	624	00	1,608 K	Host Process for Windows Services
VBoxService.exe	688	00	948 K	VirtualBox Guest Additions Service
svchost.exe	752	00	2,728 K	Host Process for Windows Services
svchost.exe	808	00	6,168 K	Host Process for Windows Services
svchost.exe	888	00	3,116 K	Host Process for Windows Services
svchost.exe	932	00	16,680 K	Host Process for Windows Services
svchost.exe	1092	00	3,156 K	Host Process for Windows Services
dwm.exe	1136	00	488 K	Desktop Window Manager
svchost.exe	1204	00	13,128 K	Host Process for Windows Services
spoolsv.exe	1328	00	1,296 K	Spooler SubSystem App
svchost.exe	1364	00	4,200 K	Host Process for Windows Services
explorer.exe	1384	00	33,680 K	Windows Explorer
WSActiveBridge.exe	1452	00	1,376 K	WSActiveBridge WebSocket Server
svchost.exe	1484	00	2,540 K	Host Process for Windows Services

Figure 4. The voice conversion software (WSActiveBridge.exe) is listening on port 45461 and 45462

Reconnaissance is the stage where attackers collect information from potential targets to help them determine what tactics will work. These new developments from the Andariel group give us an idea of their plans, although we cannot make specific assumptions about their strategy.

To stay one step ahead of threats like this, we recommend that people use layered security protection in their environments. Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security can protect users and businesses from similar threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that 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 advanced malware.

Indicators of Compromise (IoC)

IoCs	Description
cfcd391eec9fca663afd9a4a152e62af665e8f695a16537e061e924a3b63c3b9	Injected Script in May 2018
e0e30eb5e5ff1e71548c4405d04ce16b94c4cb7f8c2ed9bd75933cea53533114	Injected Script in June 2018
67a1312768c4ca3379181c0fcc1143460efcb4bff7a4774c9c775043964c0878	Injected Script in 17 July 2018
hxxp://aega[.]co[.]kr/mall/skin/skin.php	Compromised site (received information May 2018)
hxxp://www[.]peaceind[.]co[.]kr/board/icon/image.php	Compromised site (received information May 2018)

hxxp://alphap1[.]com/hdd/images/image.php	Compromised site (received information May 2018)
hxxp://adfamc[.]com/editor/sorak/image.php	Compromised site (received information June 2018)
hxxp://adfamc[.[com/editor/sorak/skin.php	Compromised site (received information 17 July 2018)