COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

Indicators of Compromise

Apr 6, 2018

This report documents Indicators of Compromise generated by Cobalt Strike during this engagement.

Summary

Hashes:	2
Domains:	1
Payloads:	1

HaveX Trojan

This payload was observed in conjunction with this actor's activities.

Portable Executable Information

Checksum:	0
Compilation Timestamp:	30 Dec 2013 07:53:48
Entry Point:	134733
Name:	Tmprovider.dll
Size:	340kb (348160 bytes)
Target Machine:	x86

This payload resides in memory pages with RWX permissions. These memory pages are not backed by a file on disk.

Contacted Hosts

Host	Port	Protocols
172.16.4.131	80	HTTP

HTTP Traffic

```
GET /include/template/isx.php HTTP/1.1
Referer: http://www.google.com
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Cookie: cFHHOdFMNrombFD0yV9bjw==
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 5.2) Java/1.5.0_08

HTTP/1.1 200 OK
Server: Apache/2.2.26 (Unix)
X-Powered-By: PHP/5.3.28
Cache-Control: no-cache
Content-Type: text/html
Keep-Alive: timeout=3, max=100
Content-Length: 238

<html><head><mega http-equiv='CACHE-CONTROL'
content='NO-CACHE'></head><body>Sorry, no data
corresponding your request.<!--havex5dOeUFrn9JjyD8B8Grev
+Pf5afc5uwcjXFkGDKm6s5N0v5JGyb9roicuNelvNGCrzC3DexfCSJd1PvDM60C86Q==havex--
></body></html>
```

Extracted Strings

```
%s <%s> (Type=%i, Access=%i, ID='%s')
%02i was terminated by ThreadManager(2)
main sort initialise ...
qsort [0x%x, 0x%x] done %d this %d
{0x%08x, 0x%08x}
Programm was started at %02i:%02i:%02i
a+
%02i:%02i:%02i.%04i:
******************************************************************************************
Start finging of LAN hosts...
Finding was fault. Unexpective error
Hosts was't found.
%O2i) [%s]
Start finging of OPC Servers...
Was found %i OPC Servers.
%i) [%s\%s]
CLSID: %s
UserType: %s
VerIndProgID: %s
OPC Servers not found. Programm finished
Start finging of OPC Tags...
[-]Threads number > Hosts number
[-]Can not get local ip
[!]Start
[+]Get WSADATA
[+]Local:
[-]Connection error
Was found %i hosts in LAN:
%s[%s]!!!EXEPTION %i!!!
final combined CRC = 0x%08x
```

File Hashes

The following file hashes were observed in conjunction with this actor's activities.

MD5 Hash	File Size
57d2195aacdd2be8805a7c0751cf1c25	14848
8d7514df3afd93932b495785b4ccbba4	15360

Domains and IP Addresses

The following domains and IP addresses were attributed to this actor.

172.16.4.131