Let's Learn: TrickBot "BazarBackdoor" Process Hollowing Injection Primer

vkremez.com/2020/04/lets-learn-trickbot-bazarbackdoor.html

Goal: Review the latest stealthy TrickBot group backdoor dubbed as "BazarBackdoor" as well as its process injection methodology approach.

> #Malware @googledocs
> 📨 tyrone.smith@mymona.uwi.edu via @SendGrid
> 📩 Re: , your report
>
> 🔗 hxxps://www.ruths-brownies.com/PreviewReport.DOC.exe
> 📁 a9952f532a7141910b2261394a52e6dc
>
> 🌐 Multiple DNS
> > bestgame.bazar
> > forgame.bazar
> > IP connections: https://t.co/bhdN0n4Fqu pic.twitter.com/leZb64pfFc
> — панкак3 (@pancak3lullz) April 20, 2020

Source:

```
Crypted Loader SHA-256:
1e123a6c5d65084ca6ea78a26ec4bebcfc4800642fec480d1ceeafb1cacaaa83
64-bit Backdoor SHA-256:
5974d938bc3bbfc69f68c979a6dc9c412970fc527500735385c33377ab30373a
```

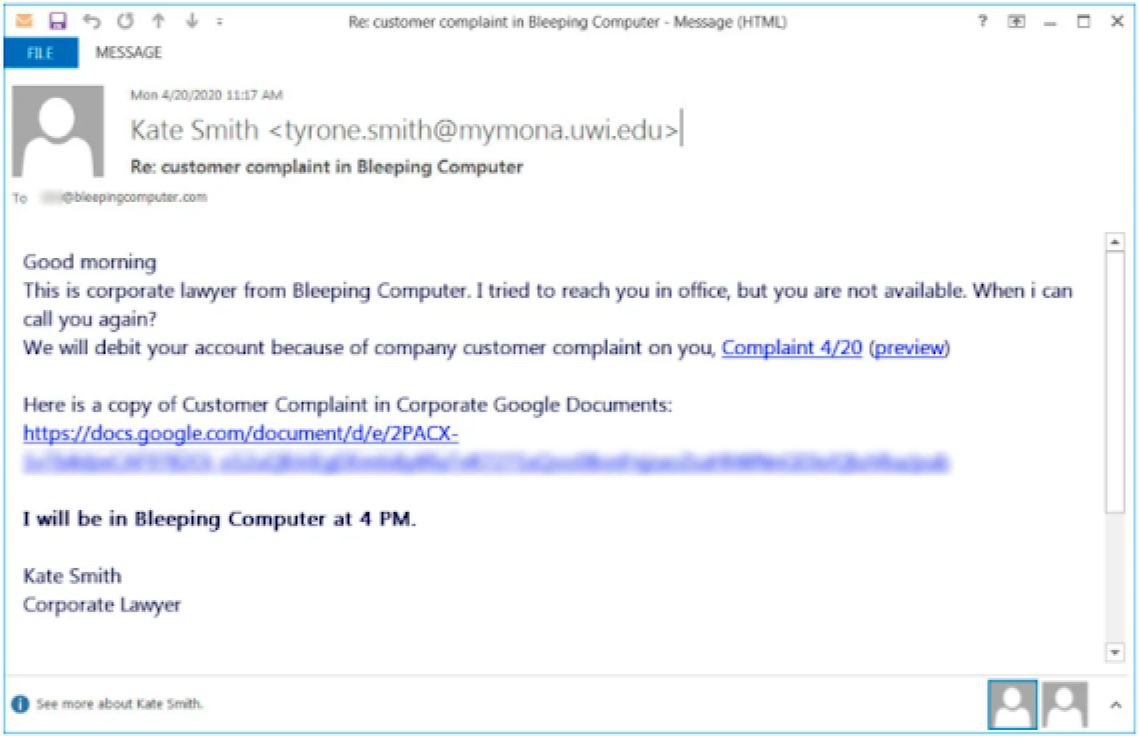
Outline:

```
I. BazarBackdoor: Background & Executive Summary
II. BazarLoader: Process Hollowing Methodology
III. BazarBackdoor: Overview
IV. Yara Signature: BazarBackdoor Payload
V. Mitre ATT&CK Framework: BazarBackdoor Payload
VI. Network JA3 Signature: BazarLoader Malware
```

I. BazarBackdoor: Background & Executive Summary

BazarBackdoor is the new stealthy covert malware leveraged for high-value targets part of the TrickBot group toolkit arsenal. For more overall information, please read the BleepingComputer report from Lawrence Abrams related to this malware functionality and discovery.
The malware was signed “VB CORPORATE PTY. LTD.” as DigiCert
The TrickBot backdoor is a lightweight malware aimed to evade detection and be lightweight.

It leverages a known TrickBot group crypter with the notable VirtualAllocExNuma API and RC4 decoder sequence.



Re: customer complaint in Bleeping Computer - Message (HTML)

Mon 4/20/2020 11:17 AM

Kate Smith <tyrone.smith@mymona.uwi.edu>

Re: customer complaint in Bleeping Computer

To [redacted]@bleepingcomputer.com

Good morning
This is corporate lawyer from Bleeping Computer. I tried to reach you in office, but you are not available. When i can call you again?
We will debit your account because of company customer complaint on you, Complaint 4/20 (preview)

Here is a copy of Customer Complaint in Corporate Google Documents:
https://docs.google.com/document/d/e/2PACX-
[redacted]

I will be in Bleeping Computer at 4 PM.

Kate Smith
Corporate Lawyer

See more about Kate Smith.

Example BazarLoader phishing email

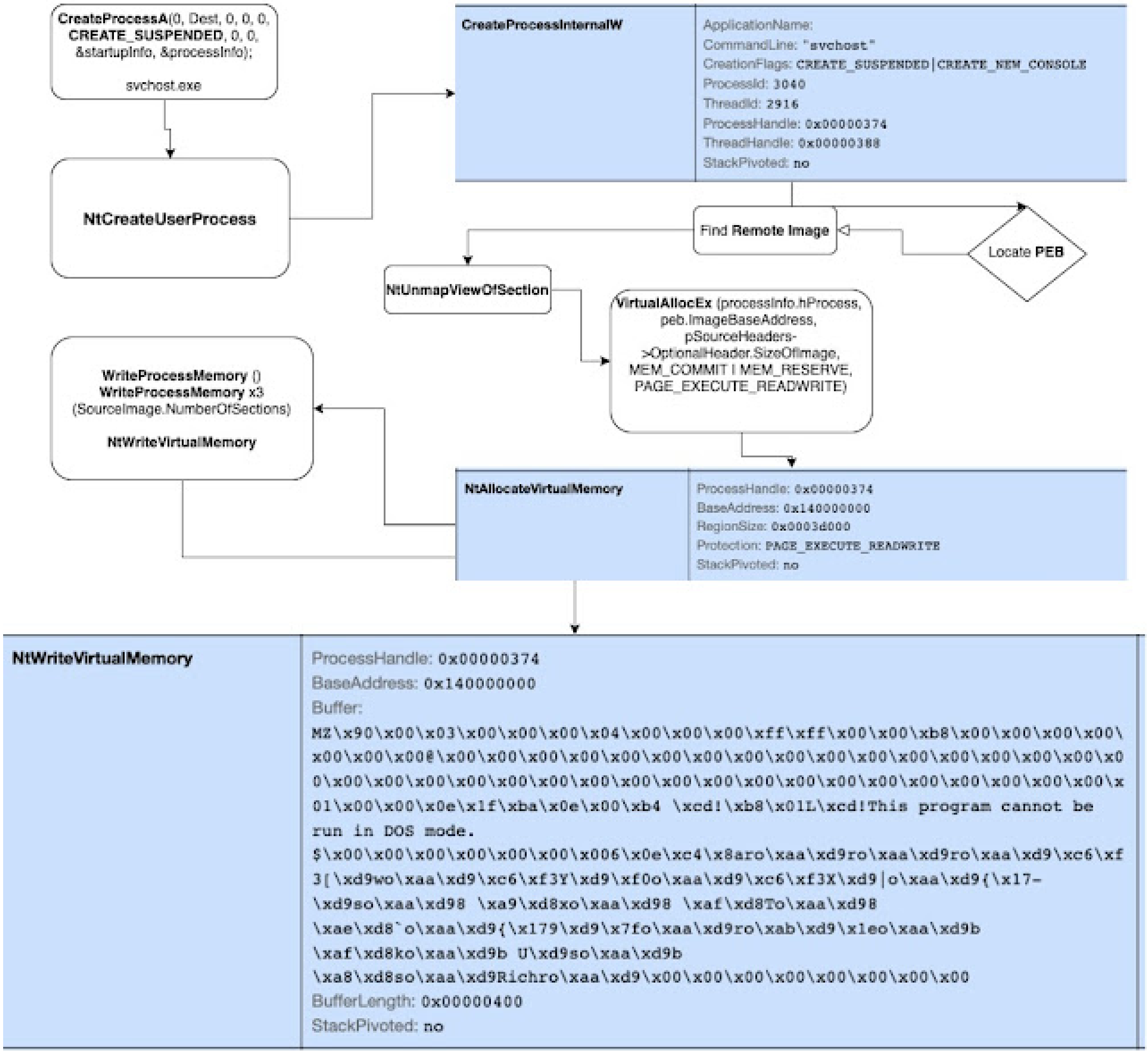
The TrickBot Anchor project and this backdoor both utilize the same Emercoin DNS for the server communication via /api/ request for the payload with architecture configuration (for example, /api/86 and /api/88). By and large, Emercoin DNS is a legitimate provider that leveraged for .bazar domain resolution.

The goal of this fileless loader and backdoor is not to elevate privileges but to avoid any detection possible staying silently and only loading extra functionality as extra features. In case they get flagged as malicious, the bot would still remain in the system.

The malware combination consists of two parts: loader and bot. The bot goal is to execute binaries, scripts, and modules, kill processes and remove itself from the compromised machine.

II. BazarLoader: Process Hollowing Methodology

The malware utilizes the process hollowing injection approach injecting the core backdoor into svchost.exe via the following sequence *CreateProcessA(0, pDestCmdLine, 0, 0, 0, CREATE_SUSPENDED, 0, 0, &startupInfo, &processInfo) -> Find PEB -> Locate Remote Image*
NtUnmapViewOfSection -> VirtualAllocEx -
> VirtualAllocEx(processInfo.hProcess, peb.ImageBaseAddress, ...,MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE) -
> WriteProcessMemory () -> WriteProcessMemory (SourceImage.NumberOfSections)


CreateProcessA(0, Dest, 0, 0, 0, CREATE_SUSPENDED, 0, 0, &startupInfo, &processInfo);
svchost.exe
NtCreateUserProcess
CreateProcessInternalW
Find Remote Image
Locate PEB
NtUnmapViewOfSection
VirtualAllocEx (processInfo.hProcess, peb.ImageBaseAddress, pSourceHeaders->OptionalHeader.SizeOfImage, MEM_COMMIT I MEM_RESERVE, PAGE_EXECUTE_READWRITE)
WriteProcessMemory ()
WriteProcessMemory x3 (SourceImage.NumberOfSections)
NtWriteVirtualMemory
NtAllocateVirtualMemory
NtWriteVirtualMemory

```
ApplicationName:
CommandLine: "svchost"
CreationFlags: CREATE_SUSPENDED|CREATE_NEW_CONSOLE
ProcessId: 3040
ThreadId: 2916
ProcessHandle: 0x00000374
ThreadHandle: 0x00000388
StackPivoted: no
```

```
ProcessHandle: 0x00000374
BaseAddress: 0x140000000
RegionSize: 0x0003d000
Protection: PAGE_EXECUTE_READWRITE
StackPivoted: no
```

```
ProcessHandle: 0x00000374
BaseAddress: 0x140000000
Buffer:
MZ\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff\x00\x00\xb8\x00\x00\x00\x00\
x00\x00\x00@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
01\x00\x00\x0e\x1f\xba\x0e\x00\xb4 \xcd!\xb8\x01L\xcd!This program cannot be
run in DOS mode.
$\x00\x00\x00\x00\x00\x00\x006\x0e\xc4\x8aro\xaa\xd9ro\xaa\xd9ro\xaa\xd9\xc6\xf
3[\xd9wo\xaa\xd9\xc6\xf3Y\xd9\xf0o\xaa\xd9\xc6\xf3X\xd9|o\xaa\xd9{\x17-
\xd9so\xaa\xd98 \xa9\xd8xo\xaa\xd98 \xaf\xd8To\xaa\xd98
\xae\xd8`o\xaa\xd9{\x179\xd9\x7fo\xaa\xd9ro\xab\xd9\x1eo\xaa\xd9b
\xaf\xd8ko\xaa\xd9b U\xd9so\xaa\xd9b
\xa8\xd8so\xaa\xd9Richro\xaa\xd9\x00\x00\x00\x00\x00\x00\x00\x00
BufferLength: 0x00000400
StackPivoted: no
```

III. BazarLoader: Host Persistence

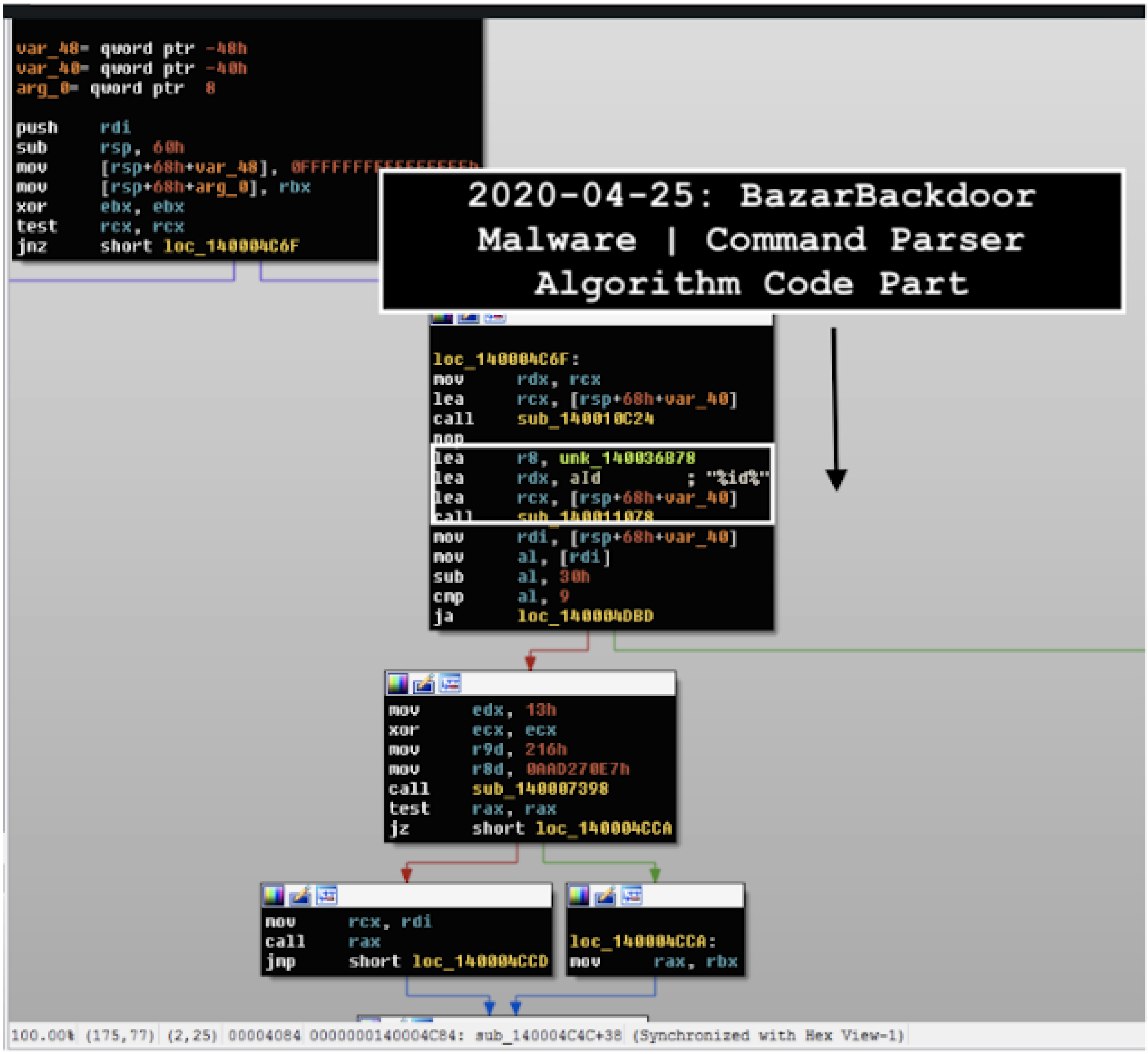
The loader adds itself to *\Software\Microsoft\Windows\CurrentVersion\Run* and uses its process key for persistence.

The malware decryption routine is as follows:

```
const char *Encrypt_Decrypter()
 {
  ...
  BYTE key = key;
  for (int i = 0; i < len; i++)
  {
   ptr[i] = ptr[i + 1] ^ key;
   key++;
  }
 }
```

IV. BazarBackdoor: Overview

The backdoor goal is to execute binaries, scripts, and modules, kill processes and remove itself from the compromised machine.



2020-04-25: BazarBackdoor Malware | Command Parser Algorithm Code Part

```
var_48= qword ptr -48h
var_40= qword ptr -40h
arg_0= qword ptr  8

push    rdi
sub     rsp, 60h
mov     [rsp+68h+var_48], 0FFFFFFFFFFFFFFFEh
mov     [rsp+68h+arg_0], rbx
xor     ebx, ebx
test    rcx, rcx
jnz     short loc_140004C6F
```

```
loc_140004C6F:
mov     rdx, rcx
lea     rcx, [rsp+68h+var_40]
call    sub_140010C24
nop
lea     r8, unk_140036B78
lea     rdx, aId        ; "%id%"
lea     rcx, [rsp+68h+var_40]
call    sub_140011078
mov     rdi, [rsp+68h+var_40]
mov     al, [rdi]
sub     al, 30h
cmp     al, 9
ja      loc_140004DBD
```

```
mov     edx, 13h
xor     ecx, ecx
mov     r9d, 216h
mov     r8d, 0AAD270E7h
call    sub_140007398
test    rax, rax
jz      short loc_140004CCA
```

```
mov     rcx, rdi
call    rax
jmp     short loc_140004CCD
```

```
loc_140004CCA:
mov     rax, rbx
```

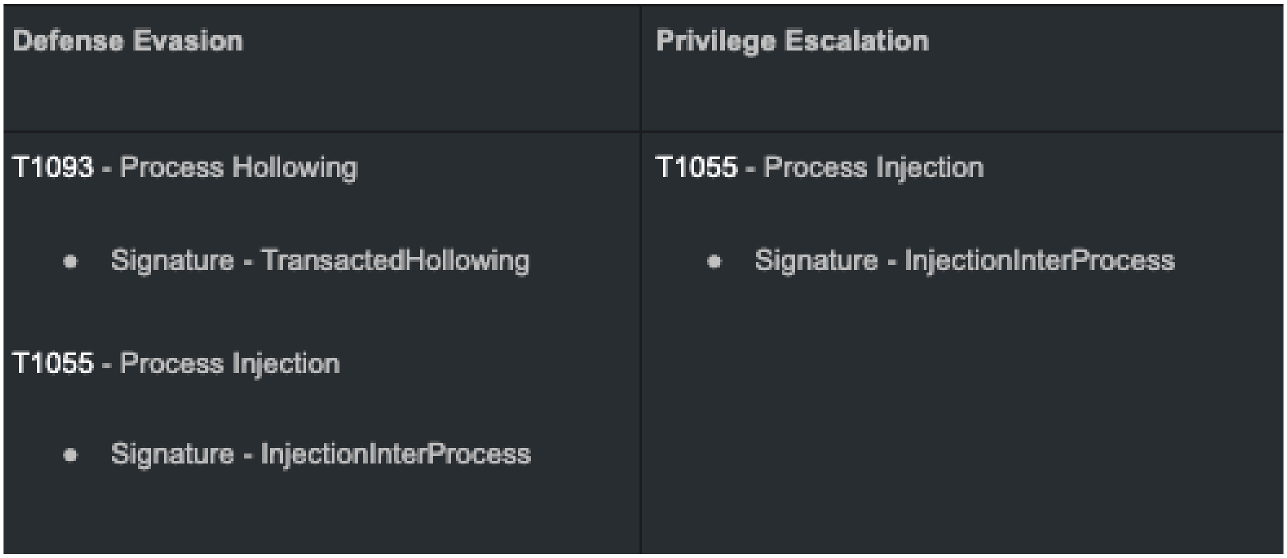
```
100.00% (175,77) (2,25) 00004084 0000000140004C84: sub_140004C4C+38 (Synchronized with Hex View-1)
```

V. Yara Signature: BazarBackdoor Payload

```
rule crime_win64_backdoor_bazarbackdoor1 {

meta:
 description = "Detects BazarBackdoor injected 64-bit malware"
 author = "@VK_Intel"
 reference = "https://twitter.com/pancak3lullz/status/1252303608747565057"
 tlp = "white"
 date = "2020-04-24"

strings:
 $str1 = "%id%"
 $str2 = "%d"

 $start = { 48 ?? ?? ?? ?? 57 48 83 ec 30 b9 01 00 00 00 e8 ?? ?? ?? ?? 84 c0 0f ??
?? ?? ?? ?? 40 32 ff 40 ?? ?? ?? ?? e8 ?? ?? ?? ?? 8a d8 8b ?? ?? ?? ?? ?? 83 f9 01
0f ?? ?? ?? ?? ?? 85 c9 75 ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48
?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? 85 c0 74 ?? b8 ff 00 00 00 e9 ?? ?? ?? ?? 48 ?? ??
?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? eb ??
40 b7 01 40 ?? ?? ?? ?? 8a cb e8 ?? ?? ?? ?? e8 ?? ?? ?? ?? 48 8b d8 48 ?? ?? ?? 74
??}
 $server = {40 53 48 83 ec 20 48 8b d9 e8 ?? ?? ?? ?? 85 c0 75 ?? 0f ?? ?? ?? ?? ??
?? 66 83 f8 50 74 ?? b9 bb 01 00 00 66 3b c1 74 ?? a8 01 74 ?? 48 8b cb e8 ?? ?? ??
?? 84 c0 75 ?? 48 8b cb e8 ?? ?? ?? ?? b8 f6 ff ff ff eb ?? 33 c0 48 83 c4 20 5b c3}

condition:
 ( uint16(0) == 0x5a4d and ( 3 of them ) ) or ( all of them )

}
```

VI. Mitre ATT&CK Framework: BazarBackdoor Payload

The mapped Mitre ATT&CK Framework is as follows:



Defense Evasion	Privilege Escalation
T1093 - Process Hollowing • Signature - TransactedHollowing T1055 - Process Injection • Signature - InjectionInterProcess	T1055 - Process Injection • Signature - InjectionInterProcess

Mitre ATT&CK Framework:

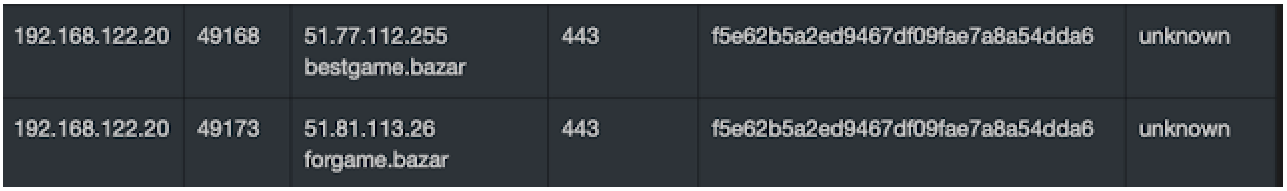
- T1093 - Process Hollowing
  Signature - TransactedHollowing
- T1055 - Process Injection

Signature - InjectionInterProcess

VII. Network JA3 Signature: BazarLoader Malware (f5e62b5a2ed9467df09fae7a8a54dda6)

The hostnames used for the command-and-control servers are:

```
forgame.bazar
bestgame.bazar
thegame.bazar
newgame.bazar
portgame.bazar
```



192.168.122.20	49168	51.77.112.255 bestgame.bazar	443	f5e62b5a2ed9467df09fae7a8a54dda6	unknown
192.168.122.20	49173	51.81.113.26 forgame.bazar	443	f5e62b5a2ed9467df09fae7a8a54dda6	unknown