← Go to listing page

APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations

Threat Actor

Threat Actor Profile

Origin: 2014

Aliases: Helix Kitten, OilRig, Greenbug

Key Target Sectors: Information Technology, Government, Military, Energy and Power, Communication, Transportation, Financial Services, Educational System

Attack Vectors: Zero Day Attacks, Data theft, Spam Email, Remote Code Execution, Living off the Land Attack, Social Engineering, Spearphishing, backdoor, Luring, Watering Hole Attack

Target Region: Western Asia, Western Europe, North America, South America, Southern Asia, South-East Asia, Africa, Eastern Europe

Malware Used: Quadagent, Twoface, Helminth, OopsIE, Karkoff, Fox Panel, HighShell, Glimpse, Webmask, RunningBee, HyperShell, ISMAgent, Poison Frog, PhpSpy, ThreeDollars, Neptun, Pickpocket, ValueVault, and Longwatch

Vulnerabilities Exploited: CVE-2017-0199 and CVE-2017-11882

Overview

APT34 is an Advanced Persistent Threat (APT) group, active since 2014. This group works on behalf of the Iranian government and has been observed targeting victims mostly across the Middle Eastern region.

They have targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has primarily focused its operations within the Middle East. This adversary was originally identified and tracked as two separate groups, OilRig and APT34. But further research and evidence revealed an overlap between their activities, and eventually, most researchers agreed to track them as a single Threat Actor. Most recently in mid-2019, Turla (Cyber-espionage group from Russia) hijacked the Infrastructure of this APT, in one of their attack campaigns.

Which organizations have they targeted?

The group was initially observed targeting financial organizations and government agencies across the Middle Eastern region and the US, but gradually it moved to other regions and sectors.

- Since 2014, the group's attacks were focused on Middle Eastern banks and government entities since 2014. Later, their primary targets changed, but the trend of targeting critical infrastructure and governmental entities remained the same.
- In October 2016, the group was observed to be targeting government entities in Middle Eastern countries and

the U.S., along with several airlines from Middle Eastern countries.

- Between 2017 to 2018, the group focused more on Western-Asian and North American organizations working in Education, Information Technology and Government sector.
- In April 2019, information leaked by elite hackers “Lab Dookhtegan” and “Mr_L4nnist3r” revealed the victim’s names as the Saudi Arabian Communications & Information Technology Commission, Dubai Statistics Association.
- In the same duration, a small handful of targets were based outside the Middle East, including a telecom company in Zimbabwe, government bodies in Albania, and South Korean gaming business.
- Most recently in June 2019, a phishing campaign was observed, targeting energy companies, government utilities, and their workers.

What is their motivation behind the attacks?

This group is known to use various malware and tools to collect strategic information that would benefit the economic and geopolitical interests of the state of Iran. Also, Iran considers cyber-attacks as an

offensive weapon against its rival countries like the United States of America and Israel. The cyberattacks linked to the group are not that advanced or sophisticated, but highly persistent with their victim choice, which is directly or indirectly connected to Iran's military, financial, and political interests.

Modus Operandi

Since 2014, the group is known to be using Microsoft Excel macros, PowerShell-based exploits, and social engineering to gain access to its targets. They use phishing emails to deliver weaponized Microsoft Excel documents, and most of their malware infect the target system with VisualBasic and PowerShell (.ps1) scripts.

- Between 2014 to 2016, the group's attack campaigns targeted banks and technology organizations in Saudi Arabia with phishing emails that included weaponized Microsoft Excel attachments. One spam email had a legitimate conversation between employees, which was used as a lure, and forwarded to other employees with a weaponized attachment. Other related campaign phishing emails used job or service offering.
- In early-2017, the group was observed again, using a fake Juniper Networks VPN portal and few fake University of

Oxford websites to deliver malware to the victims. The group registered four domain names belonging to Oxford University (including oxford-careers[.]com, oxford[.]in and oxford-employee[.]com).

- In April 2017, they launched a massive cyber-espionage campaign against major Israeli institutions and government officials. They exploited CVE-2017-0199 remote code execution vulnerability in the Windows Object Linking and Embedding (OLE) application programming interface. They managed to target the victims before Microsoft issued a security update, and organizations rolled out the patch.
- In May 2017, they expanded their geographical range with hundreds of new attacks targeting several militaries, financial and energy businesses in Europe as well as the United States. In these attacks, they collaborated with Russian hackers-for-hire.
- In Sep. 2017, an analysis done by a security firm on Two-face (web shell) disclosed a complex malicious infrastructure that was targeting Israeli institutions earlier in April. The links between TwoFace and five other web shells were found, including RunningBee, PuTTY Link (plink) and

Share Blog Post

RGDoor (for Microsoft IIS).

- In Oct. 2017, the group developed the "Agent Injector" (Trojan with the specific purpose of installing the ISMAgent backdoor) to target an organization within the United Arab Emirates government. The attack used a spearphishing spam email that had a subject of 'Importan Issue'. The group was also found to be using CVE-2017-11882, an Office vulnerability patched by Microsoft on November 14, 2017.
- On January 8, 2018, the group launched an attack on an insurance agency based in the Middle East. They tried to deliver a new Trojan called OopsIE, via using a variant of the ThreeDollars delivery document. They sent two emails to two separate email addresses within the same organization. The email address was linked with the Lebanese domain of a major global financial institution.
- In Feb 2018, it was discovered that threat actor dubbed 'Chafer' (having an association or related to APT34) successfully compromised one of the biggest telecom firms in the Middle East using leaked NSA hacking tools.
- In March 2018, the group improved their Critical Infrastructure attacks with new off-the-shelf tools, dual-purpose utilities. They were found to be using earlier unseen malware, that uses

SmartFile, Google Drive, and internet server API (ISAPI) filters for compromising Microsoft Internet Information Services (IIS) servers.

- In July 2018, they launched multiple attacks using spearphishing email (having attached PhpSpy and QuadAgent backdoor) to target an unnamed technology services provider, the Lebanese intelligence agency, and healthcare facilities in Saudi Arabia. Their initial infection paths were based on watering hole attacks using compromised web servers. In Sep., they deployed a new variant of their OopsIE Trojan that came with new evasion techniques.
- In the same month, they also conducted at least one attack campaign containing an updated variant of the BondUpdater Trojan (uses DNS tunneling) as its final payload.
- In Nov. 2018, new information shed light on the fact that the group tests their malicious documents before they are being used in their attacks.
- In April 2019, a group that calls itself Lab Dookhtegan exposed several tools (Poison Frog, Glimpse, HyperShell, HighShell, Fox Panel, and Webmask) used by this group.
- In the same month, a DNSpionage malware campaign was also discovered,

using a new malware called 'Karkoff.' The malware was delivered via an Excel document that included malicious macros. They also created a new remote administration tool that supported HTTP and DNS communication.

- Most recently in June 2019, a Russian cyber-espionage group "Turla" was discovered to be using attack infrastructure belonging to APT34. The infrastructure was used to deliver a backdoor called "Neptun," installed on Microsoft Exchange servers.
- Also in June, a phishing campaign was observed asking victims to join their social network. This time the group masqueraded as a Cambridge University lecturer, also setting up a LinkedIn page in order to gain victims' trust. From there they asked victims to open malicious documents. In this phishing campaign, three new malware families were detected, named as Pickpocket, ValueVault, and Longwatch.

Known tools and malware

This group is known to use multiple custom malware and tools for stealing intellectual information, lateral movement, and getting an initial foothold into the targeted network.

Malicious programs used by APT34

- **Twoface -** A web shell, which is used to harvest credentials
- **Powruner -** A backdoor known to be used by APT34.
- **RGDoor -** An Internet Information Services backdoor which is created using C++.
- **Helminth -** A Trojan that is developed to target the Windows platform.
- **OopsIE -** A Trojan deployed and known to be used by APT34.
- **Karkoff -** A malware designed to execute code remotely on compromised hosts.
- **ISMAgent -** A backdoor which has a sophisticated architecture and contains anti-analysis techniques.
- **Poison Frog -** A backdoor used along with BondUpdater tool.
- **PhpSpy -** A backdoor used for an initial foothold in the targeted network.
- **Neptun -** A backdoor installed on Microsoft Exchange servers as a service.
- **Pickpocket -** It is a browser credential-theft tool.
- **ValueVault -** It is used to extract and view the credentials stored in the Windows Vault.
- **LongWatch -** A Pickpocket variant, and browser credential-theft tool.

Custom tools used by APT34

- **Quadagent -** A PowerShell backdoor tool, that is attributed to APT34.
- **ThreeDollars -** A delivery document, which is identified as part of the OilRig toolset.
- **Fox Panel -** A hacking tool is known to be linked and used by APT34
- **HighShell -** A web shell-based TwoFace payload used by APT34.
- **Glimpse -** A tool within the data dump, related to the updated BondUpdater tool.
- **Webmask -** A series of scripts specifically meant to perform DNS hijacking.
- **RunningBee -** A web-based TwoFace payload used by APT34.
- **HyperShell -** A TwoFace loader known to used by APT34.

Known Zero Days Vulnerabilities

- **Microsoft Office Remote Code Execution Vulnerability (CVE-2017-0199) -** A remote code-execution vulnerability in Microsoft Office/Wordpad.
- **Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882) -** A memory-corruption vulnerability in Microsoft Office.

Attribution

The use of infrastructure linked to Iranian operations, alignment, and timing with the national interests of Iran lead to the conclusion that this group acts or works on behalf of the Iranian government. The persistency in the targets of their attack, which are mostly from middle-east countries, also proves the fact that the cyberattacks originated from Iran. Most of their cyber campaigns became active when there was a holiday in Iran, and targeted specific countries with conflict of interest with Iran.

Prevention

Organizations and security experts should review the Indicators of Compromise (IoCs) and use them with their Endpoint Detection and Response (EDR) tool. Organizations should also consider having threat intel ingestion for their existing investments in the stack of security tools like Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), etc. with support for automated enrichment from external sources, which would ensure protection from latest threats across the industry. The security experts must understand the fact that fully up-to-date antivirus (AV) or reliable antivirus software do not provide 100% protection

against sophisticated attacks from threats like APT34. For adequate protection, they need a layered approach to their endpoint security. Ideally, these layers must combine solutions based on dynamic security policy (e.g., behavioral-based Firewalls, Data Loss Prevention systems) as well as the control-based security policy (e.g., whitelisting, application control). Enterprise networks with endpoint security solutions based on the OS-Centric security approach are more secure against the new types of APT34 attacks. The OS-centric security solutions focus on the final stage of the attack kill chain, and intended damage, so it provides better protection no matter what attack vector or method is used.

Indicators of Compromise

Iranian Intelligence Server

185[.]56[.]91[.]61
46[.]165[.]246[.]196
185[.]236[.]76[.]80
185[.]236[.]77[.]17
185[.]181[.]8.252
185[.]191[.]228[.]103
70[.]36[.]107[.]34
109[.]236[.]85[.]129
185[.]15[.]247[.]140
185[.]181[.]8.158
178[.]32[.]127[.]230
146[.]112[.]61[.]108

23[.]106[.]215[.]76
185[.]20[.]187[.]8
95[.]168[.]176[.]172
173[.]234[.]153[.]194
173[.]234[.]153[.]201
172[.]241[.]140[.]238
23[.]19[.]226[.]69 185.
161[.]211[.]86
185[.]174[.]100[.]56
194[.]9.177[.]15
185[.]140[.]249[.]63
81[.]17[.]56[.]249
213[.]227[.]140[.]32
46[.]105[.]251[.]42
185[.]140[.]249[.]157
198[.]143[.]182[.]22
213[.]202[.]217[.]9
158[.]69[.]57[.]62
168[.]187[.]92[.]92
38[.]132[.]124[.]153
176[.]9.164[.]215
88[.]99[.]246[.]174
190[.]2.142[.]59
103[.]102[.]44[.]181
217[.]182[.]217[.]122
46[.]4.69[.]52
185[.]227[.]108[.]35
172[.]81[.]134[.]226
103[.]102[.]45[.]14
95[.]168[.]176[.]173
142[.]234[.]200[.]99
194[.]9.179[.]23
194[.]9.178[.]10

185[.]174[.]102[.]14
185[.]236[.]76[.]35
185[.]236[.]77[.]75
185[.]161[.]209[.]157
185[.]236[.]76[.]59
185[.]236[.]78[.]217
23[.]227[.]201[.]6
185[.]236[.]78[.]63

IoCs of Leaked Hacking Tools (April 219)

SHA256

27e03b98ae0f6f2650f378e9292384f1350f95
ee4f3ac009e0113a8d9e2e14ed
b1d621091740e62c84fc8c62bcdad07873c8b
61b83faba36097ef150fd6ec768
2943e69e6c34232dee3236ced38d41d37878
4a317eeaf6b90482014210fcd459
07e791d18ea8f2f7ede2962522626b43f28cb
242873a7bd55fff4feb91299741
dd6d7af00ef4ca89a319a230cdd094275c3a1
d365807fe5b34133324bdaa0229
3ca3a957c526eaeabcf17b0b2cd345c0fffab5
49adfdf04470b6983b87f7ec62
c9d5dc956841e000bfd8762e2f0b48b66c79b
79500e894b4efa7fb9ba17e4e9e
a6a0fbfee08367046d3d26fb4b4cf7779f7fb6
eaf7e60e1d9b6bf31c5be5b63e
Fe1b011fe089969d960d2dce2a61020725a02
e15dbc812ee6b6ecc6a98875392

Shells

hxxps://202[.]183[.]235[.]31/owa/auth/signo

ut[.]aspx
hxxps://202[.]183[.]235[.]4/owa/auth/signout
[.]aspx
hxxps://122[.]146[.]71[.]136/owa/auth/error3
[.]aspx
hxxps://59[.]124[.]43[.]229/owa/auth/error0[.
]aspx
hxxps://202[.]134[.]62[.]169/owa/auth/signin
[.]aspx
hxxps://202[.]164[.]27[.]206/owa/auth/signo
ut[.]aspx
hxxps://213[.]14[.]218[.]51/owa/auth/logon[.]
aspx
hxxps://88[.]255[.]182[.]69/owa/auth/getidto
ken[.]aspx
hxxps://95[.]0.139[.]4/owa/auth/logon[.]aspx
hxxps://1[.]202[.]179[.]13/owa/auth/error1[.]
aspx
hxxps://1[.]202[.]179[.]14/owa/auth/error1[.]
aspx
hxxps://114[.]255[.]190[.]1/owa/auth/error1[.
]aspx
hxxps://180[.]166[.]27[.]217/owa/auth/error3
[.]aspx
hxxps://180[.]169[.]13[.]230/owa/auth/error1
[.]aspx
hxxps://210[.]22[.]172[.]26/owa/auth/error1[.
]aspx
hxxps://221[.]5.148[.]230/owa/auth/outlook[.
]aspx
hxxps://222[.]178[.]70[.]8/owa/auth/outlook[
.]aspx
hxxps://222[.]66[.]8.76/owa/auth/error1[.]as

px
hxxps://58[.]210[.]216[.]113/owa/auth/error1[.]aspx
hxxps://60[.]247[.]31[.]237/owa/auth/error3[.]aspx
hxxps://60[.]247[.]31[.]237/owa/auth/logoff[.]aspx
hxxps://202[.]104[.]127[.]218/owa/auth/error1[.]aspx
hxxps://202[.]104[.]127[.]218/owa/auth/exppw[.]aspx
hxxps://132[.]68[.]32[.]165/owa/auth/logout[.]aspx
hxxps://132[.]68[.]32[.]165/owa/auth/signout[.]aspx
hxxps://209[.]88[.]89[.]35/owa/auth/logout[.]aspx
hxxps://114[.]198[.]235[.]22/owa/auth/login[.]aspx
hxxps://114[.]198[.]237[.]3/owa/auth/login[.]aspx
hxxps://185[.]10[.]115[.]199/owa/auth/logout[.]aspx
hxxps://195[.]88[.]204[.]17/owa/auth/logout[.]aspx
hxxps://46[.]235[.]95[.]125/owa/auth/signin[.]aspx
hxxps://51[.]211[.]184[.]170/owa/auth/owaauth[.]aspx
hxxps://91[.]195[.]89[.]155/owa/auth/signin[.]aspx
hxxps://82[.]178[.]124[.]59/owa/auth/gettokenid[.]aspx

hxxps://83[.]244[.]91[.]132/owa/auth/logon[.]aspx
hxxps://195[.]12[.]113[.]50/owa/auth/error3[.]aspx
hxxps://78[.]100[.]87[.]199/owa/auth/logon[.]aspx
hxxps://110[.]74[.]202[.]90/owa/auth/errorff[.]aspx
hxxps://211[.]238[.]138[.]68/owa/auth/error1[.]aspx
hxxps://168[.]63[.]221[.]220/owa/auth/error3[.]aspx
hxZps://213[.]189[.]82[.]221/owa/auth/errorff[.]aspx
hxxps://205[.]177[.]180[.]161/owa/auth/erroref[.]aspx
hxxps://77[.]42[.]251[.]125/owa/auth/logout[.]aspx
hxxps://202[.]175[.]114[.]11/owa/auth/error1[.]aspx
hxxps://202[.]175[.]31[.]141/owa/auth/error3[.]aspx
hxxps://213[.]131[.]83[.]73/owa/auth/error4[.]aspx
hxxps://187[.]174[.]201[.]179/owa/auth/error1[.]aspx
hxxps://200[.]33[.]162[.]13/owa/auth/error3[.]aspx
hxxps://202[.]70[.]34[.]68/owa/auth/error0[.]aspx
hxxps://202[.]70[.]34[.]68/owa/auth/error1[.]aspx
hxxps://197[.]253[.]14[.]10/owa/auth/logout[.]

]aspx
hxxps://41[.]203[.]90[.]221/owa/auth/logout[.]aspx
hxxp://www[.]abudhabiairport[.]ae/english/resources[.]aspx
hxxps://mailkw[.]agility[.]com/owa/auth/RedirSuiteService[.]aspx
hxxp://www[.]ajfd[.]gov[.]ae/_layouts/workpage[.]aspx
hxxps://mail[.]alfuttaim[.]ae/owa/auth/change_password[.]aspx
hxxps://mail[.]alraidah[.]com[.]sa/owa/auth/GetLoginToken[.]aspx
hxxp://www[.]alraidah[.]com[.]sa/_layouts/WrkSetlan[.]aspx
hxxps://webmail[.]alsalam[.]aero/owa/auth/EventClass[.]aspx
hxxp://www[.]alraidah[.]com[.]sa/_layouts/WrkSetlan[.]aspx
hxxps://webmail[.]alsalam[.]aero/owa/auth/EventClass[.]aspx
hxxps://webmail[.]bix[.]bh/owa/auth/Timeoutctl[.]aspx
hxxps://webmail[.]bix[.]bh/owa/auth/EventClass[.]aspx
hxxps://webmail[.]bix[.]bh/ecp/auth/EventClass[.]aspx
hxxps://webmail[.]citc[.]gov[.]sa/owa/auth/timeout[.]aspx
hxxps://mail[.]cma[.]org[.]sa/owa/auth/signin[.]aspx
hxxps://mail[.]dallah-hospital[.]com/owa/auth/getidtokens[.]aspx

hxxps://webmail[.]dha[.]gov[.]ae/owa/auth/outlookservice[.]aspx
hxxps://webmail[.]dnrd[.]ae/owa/auth/getidtoken[.]aspx
hxxp://dnrd[.]ae:8080/_layouts/WrkStatLog[.]aspx
hxxps://www[.]dns[.]jo/statistic[.]aspx
hxxps://webmail[.]dsc[.]gov[.]ae/owa/auth/outlooklogonservice[.]aspx
hxxps://e-albania[.]al/dptaktkonstatim[.]aspx
hxxps://owa[.]e-albania[.]al/owa/auth/outlookdn[.]aspx
hxxps://webmail[.]eminsco[.]com/owa/auth/outlookfilles[.]aspx
hxxps://webmail[.]eminsco[.]com/owa/auth/OutlookCName[.]aspx
hxxps://webmail[.]emiratesid[.]ae/owa/auth/RedirSuiteService[.]aspx
hxxps://mailarchive[.]emiratesid[.]ae/EnterpriseVault/js/jquery[.]aspx
hxxps://webmail[.]emiratesid[.]ae/owa/auth/handlerservice[.]aspx
hxxp://staging[.]forus[.]jo/_layouts/explainedit[.]aspx
hxxps://government[.]ae/tax[.]aspx
hxxps://formerst[.]gulfair[.]com/GFSTMSSSPR/webform[.]aspx
hxxps://webmail[.]ictfund[.]gov[.]ae/owa/auth/owaauth[.]aspx
hxxps://jaf[.]mil[.]jo/ShowContents[.]aspx
hxxp://www[.]marubi[.]gov[.]al/aspx/viewpercthesaurus[.]aspx
hxxps://mail[.]mindware[.]ae/owa/auth/outl

ooktoken[.]aspx
hxxps://mail[.]mis[.]com[.]sa/owa/auth/Redirect[.]aspx
hxxps://webmail[.]moe[.]gov[.]sa/owa/auth/redireservice[.]aspx
hxxps://webmail[.]moe[.]gov[.]sa/owa/auth/redirectcache[.]aspx
hxxps://gis[.]moei[.]gov[.]ae/petrol[.]aspx
hxxps://gis[.]moenr[.]gov[.]ae/petrol[.]aspx
hxxps://m[.]murasalaty[.]moenr[.]gov[.]ae/signproces[.]aspx
hxxps://mail[.]mofa[.]gov[.]iq/owa/auth/RedirSuiteService[.]aspx
hxxp://ictinfo[.]moict[.]gov[.]jo/DI7Web/libraries/aspx/RegStructures[.]aspx
hxxp://www[.]mpwh[.]gov[.]jo/_layouts/CreateAdAccounts[.]aspx
hxxps://mail[.]mygov[.]ae/owa/auth/owalogin[.]aspx
hxxps://ksa[.]olayan[.]net/owa/auth/signin[.]aspx
hxxps://mail[.]omantourism[.]gov[.]om/owa/auth/GetTokenId[.]aspx
hxxps://email[.]omnix-group[.]com/owa/auth/signon[.]aspx
hxxps://mail[.]orange-jtg[.]jo/OWA/auth/signin[.]aspx
hxxp://fwx1[.]petra[.]gov[.]jo/SEDCOWebServer/global[.]aspx
hxxp://fwx1[.]petranews[.]gov[.]jo/SEDCOWebServer/content/rtl/QualityControl[.]aspx
hxxps://webmail[.]presflt[.]ae/owa/auth/logontimeout[.]aspx

hxxps://webmail[.]qchem[.]com/OWA/auth/RedirectCache[.]aspx
hxxps://meet[.]saudiairlines[.]com/ClientResourceHandler[.]aspx
hxxps://mail[.]soc[.]mil[.]ae/owa/auth/expirepw[.]aspx
hxxps://email[.]ssc[.]gov[.]jo/owa/auth/signin[.]aspx
hxxps://mail[.]sts[.]com[.]jo/owa/auth/signout[.]aspx
hxxp://www[.]sts[.]com[.]jo/_layouts/15/moveresults[.]aspx
hxxps://mail[.]tameen[.]ae/owa/auth/outlooklogon[.]aspx
hxxps://webmail[.]tra[.]gov[.]ae/owa/auth/outlookdn[.]aspx
hxxp://bulksms[.]umniah[.]com/gmgweb/MSGTypesValid[.]aspx
hxxps://evserver[.]umniah[.]com/index[.]aspx
hxxps://email[.]umniah[.]com/owa/auth/redirSuite[.]aspx
hxxps://webmail[.]gov[.]jo/owa/auth/getidtokens[.]aspx
hxxps://www[.]tra[.]gov[.]ae/signin[.]aspx
hxxps://www[.]zakatfund[.]gov[.]ae/zfp/web/tofollowup[.]aspx
hxxps://mail[.]zayed[.]org[.]ae/owa/auth/espw[.]aspx
hxxps://mail[.]primus[.]com[.]jo/owa/auth/getidtoken[.]aspx

C2 Servers

185[.]56[.]91[.]61
46[.]165[.]246[.]196
185[.]236[.]76[.]80
185[.]236[.]77[.]17
185[.]181[.]8.252
185[.]191[.]228[.]103
70[.]36[.]107[.]34
109[.]236[.]85[.]129
185[.]15[.]247[.]140
185[.]181[.]8.158
178[.]32[.]127[.]230
146[.]112[.]61[.]108
23[.]106[.]215[.]76
185[.]20[.]187[.]8
95[.]168[.]176[.]172
173[.]234[.]153[.]194
173[.]234[.]153[.]201
172[.]241[.]140[.]238
23[.]19[.]226[.]69
185[.]161[.]211[.]86
185[.]174[.]100[.]56
194[.]9.177[.]15
185[.]140[.]249[.]63
81[.]17[.]56[.]249
213[.]227[.]140[.]32
46[.]105[.]251[.]42
185[.]140[.]249[.]157
198[.]143[.]182[.]22
213[.]202[.]217[.]9
158[.]69[.]57[.]62
168[.]187[.]92[.]92
38[.]132[.]124[.]153
176[.]9.164[.]215

88[.]99[.]246[.]174
190[.]2.142[.]59
103[.]102[.]44[.]181
217[.]182[.]217[.]122
46[.]4.69[.]52
185[.]227[.]108[.]35
172[.]81[.]134[.]226
103[.]102[.]45[.]14
95[.]168[.]176[.]173
142[.]234[.]200[.]99
194[.]9.179[.]23
194[.]9.178[.]10
185[.]174[.]102[.]14
185[.]236[.]76[.]35
185[.]236[.]77[.]75
185[.]161[.]209[.]157
185[.]236[.]76[.]59
185[.]236[.]78[.]217
23[.]227[.]201[.]6
185[.]236[.]78[.]63

TAGS

helix kitten greenbug oilrig iran apt34

Posted on: August 22, 2019

← PREVIOUS
Turning the Tables on Threat Actors by L...

→ NEXT
List of Data Breaches, Malware, Vul...