

Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations

By Insikt Group®



Insikt Group® researchers used proprietary methods, including Recorded Future Network Traffic Analysis and Recorded Future Domain Analysis, along with common analytical techniques, to profile Iranian cyberespionage threat actor APT33 (Elfin) and determine whether the public exposure of their TTPs in March 2019 impacted their operations.

Data sources include the Recorded Future® Platform, Farsight Security's DNSDB, ReversingLabs, VirusTotal, Shodan, and common OSINT techniques.

This report will be of greatest interest to those interested in Middle Eastern geopolitics, as well as network defenders of organizations with a presence in the Middle East or in industries targeted by APT33, such as aerospace and defense, energy, finance, telecommunications, and manufacturing.

This research is based on data collected between February 10, 2019 and June 6, 2019.

Executive Summary

The United States and Iran continue to escalate tensions, most recently [accelerating rhetoric](#) and [actions](#) in the Strait of Hormuz, but also in the cyber domain. Over the past three months, Recorded Future's Insikt Group has observed an increase in APT33's (also known as Elfin) infrastructure building and targeting activity, and on June 21, 2019, [Yahoo! News reported](#) that the U.S. Cyber Command launched cyberattacks on an "Iranian spy group."

Iranian state-sponsored threat actor APT33 has been conducting cyberespionage activity since [at least 2013](#), predominantly targeting nations in the Middle East, but also notably targeting U.S., South Korean, and European commercial entities across a wide variety of sectors.

Insikt Group researchers used proprietary methods, including Recorded Future Domain Analysis and Recorded Future Network Traffic Analysis, along with other common analytical approaches, to profile [recently reported](#) Iranian threat actor APT33's domain and hosting infrastructure in an effort to identify recent activity and better understand the group's tactics, techniques, and procedures (TTPs).

Our research found that APT33, or a closely aligned threat actor, continues to conduct and prepare for widespread cyberespionage activity, with over 1,200 domains used since March 28, 2019 and with a strong emphasis on using commodity malware. Commodity malware is an attractive option for nation-state threat actors who wish to conduct computer network operations at scale and hide in plain sight among the noise of other threat actor activities, thus hindering attribution efforts.

The [targeting](#) of mainly Saudi Arabian organizations across a wide variety of industries aligns with historical targeting patterns for the group, which appear undeterred following previous exposés of their activity. Western and Saudi — both public and private sector — organizations in industries that have been historically targeted by APT33 should be monitoring geopolitical developments and increasing the scrutiny of operational security controls focusing on detection and remediation of initial unauthorized access, specifically from phishing campaigns, webshells, and third-party (vendor and supplier) relationships. Additionally, real-time security intelligence should be used to improve hunting in internal network and host-based telemetry.

Key Judgments

- In response to the [publication](#) of operations in late March 2019, domains associated with suspected APT33 activity were parked or changed to new hosting providers.
- APT33, or a closely aligned threat actor, continues to control C2 domains in bulk.
 - Over 1,200 domains have been in use since March 28, 2019 alone.
 - 728 of these were identified communicating with infected hosts.
 - 575 of the 728 domains were observed communicating with hosts infected by one of 19 mostly publicly available RATs.
- Almost 60% of the suspected APT33 domains that were classified to malware families related to njRAT infections, a RAT not previously associated with APT33 activity. Other commodity RAT malware families, such as AdwindRAT and RevengeRAT, were also linked to suspected APT33 domain activity.

- We assess with medium confidence that APT33, or a closely aligned threat actor, has targeted the following organizations since the disclosures in late March:
 - A conglomerate headquartered in Saudi Arabia, with businesses in the engineering and construction, utilities, technology, retail, aviation, and finance sectors
 - Two Saudi healthcare organizations
 - A Saudi company in the metals industry
 - An Indian mass media company
 - A delegation from a diplomatic institution
- We assess that the recent reporting on links between the Nasr Institute and Kavosh Security Group, as well as technical and persona analysis, overlaps among APT33, APT35, and MUDDYWATER, and is probably a result of the tiered structure that Iran utilizes to manage cyber operations.

Background

APT33 is an Iranian state-sponsored threat actor that has engaged in cyberespionage activities since at least 2013. They have typically used [commodity malware](#) and possess an [expansive network infrastructure](#) that enables them to scale their operations for victim targeting. Historically, this targeting has focused on the aerospace and defense industries, as well as the oil and gas industry, with a strong focus on companies based in Saudi Arabia. [Symantec's Elfin report](#) denoted additional targeting of the engineering, chemical, research, finance, IT, and healthcare sectors. Recorded Future's Insikt Group has been monitoring APT33 activity, beginning with research published in October 2017, which revealed new infrastructure, malware hashes, and TTPs relating to the threat actor(s).

Threat Analysis

On March 27, 2019, Symantec published research titled, "[Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.](#)" The report outlined a three-year APT33 cyberespionage campaign. Using the IP addresses and malware hashes provided in that research, Insikt Group researchers conducted a follow-up analysis of the malicious domains used by APT33 to determine two things:

1. Whether or not APT33 had continued their activities, and if so, if they had changed TTPs in response to the publication
2. Whether or not there were any previously unreported historic activities conducted by the group that were worthy of publication

Nasr Institute and Kavosh Redux

In our previous report, "[Iran's Hacker Hierarchy Exposed](#)," we concluded that the exposure of one APT33 contractor, the Nasr Institute, by FireEye in 2017, along with our intelligence on the composition and motivations of the Iranian hacker community, pointed to a tiered structure within Iran's state-sponsored offensive cyber program. We assessed that many

According to a sensitive Insikt Group source who provided information for previous research, these organizations employed a mid-level tier of ideologically aligned task managers responsible for the compartmentalized tasking of over 50 contracting organizations, who conducted activities such as vulnerability research, exploit development, reconnaissance, and the conducting of network intrusions or attacks. Each of these discrete components, in developing an offensive cyber capability, were purposefully assigned to different contracting groups to protect the integrity of overarching operations and to ensure the IRGC and/or MOIS retained control of operations and mitigated the risk from rogue hackers.

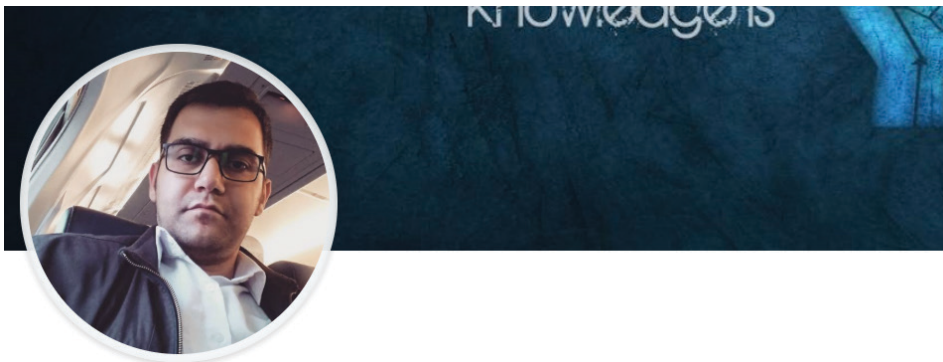


Obfuscating Iranian government involvement in offensive campaigns.

FireEye also noted in their 2017 report that the online handle “xman_1365_x,” found within the PDB path in an APT33 TURNEDUP backdoor sample, belonged to an individual at the Nasr Institute. The same handle was then linked to destructive operations using NewsBeef and StoneDrill malware families. Then, in March 2017, [researchers linked](#) StoneDrill to the Shamoan 2 operation and to the APT35 (also known as Charming Kitten, Newscaster, or NewBeef) threat actor.

Our [previous analyses](#) showed that the person behind the “xman_1365_x” handle self-identified on Iranian hacking forums as Mahdi Honarvar from Mashhad, with [speculation](#) that he was also affiliated with the Kavosh Security Center since around 2017.

Kavosh's role within the Iranian cyber ecosystem was further uncovered by Group-IB's [recent analysis](#) detailing that Kavosh was the employer for "Nima Nikjoo" between 2006 and 2014. Their analysis concluded that a March 2019 campaign targeting a Turkish military electronics manufacturer was perpetrated by another Iranian threat actor, MUDDYWATER. MUDDYWATER used the POWERSTATS backdoor, proliferated in maldocs that contained metadata revealing the author as "Gladiator_CRK," with a possible name of "Nima." Additionally, an email address suspected to be related, "gladiator_cracker@yahoo.com," was associated with "نیمای نیکجو," which translates to "Nima Nickjou," in a 2014 [blog](#) that exposed the names and email addresses of individuals allegedly employed at the Nasr Institute. Another [research blog](#) authored by pseudonym "0xffff0800" corroborated some of these findings and revealed "Nima Nikjoo" to be "Nima Nikjoo Tabrizi."



Nima Nikjoo

Malware Analyst & Vulnerability Researcher at Freelancer

Iran · See 500+ connections · [See contact info](#)

LinkedIn profile picture of suspected APT33 threat actor Nima Nikjoo Tabrizi. (Accessed on June 14, 2019)

Who Is Nima Nikjoo Tabrizi?

OSINT reveals there is an active LinkedIn account and other active social media accounts in the name of Nima Nikjoo Tabrizi, claiming that he is a reverse engineer and malware analyst at Symantec. Symantec, however, has confirmed to Recorded Future that Tabrizi has never worked for them:

"We have been aware of this individual for a long time. Nima Nikjoo is not a Symantec employee and we have no record of an individual by this name working at Symantec."

Having been exposed working for the Nasr Institute, a government organization, and the [Kavosh Security Center](#), which has strong associations with Iranian state-sponsored cyberespionage activity, we assess with high confidence that Tabrizi is engaged in cyberespionage activity on behalf of the Iranian state.

Experience



Malware Analyst and Exploit Developer

Freelancer

Apr 2019 – Present · 3 mos

Tehran Province, Iran

- Malware Analysis
- Vulnerability Researcher and Exploit Developer
- Low-Level System Programming
- CyberSecurity Consulting



Malware Analysis & Software Security Assessor

Symantec

Aug 2014 – Present · 4 yrs 11 mos

Remote Working for UAE Representation

- 1.Engine Security Examination
- 2.Provide some restricted information from Dark Web and underground areas
- 3.Limited Malware Analysis Job
- 4.Security Risk Management And Threat Consulting

[See less](#)

Employment history of suspected APT33 threat actor Nima Nikjoo Tabrizi.

Based on this information, it is possible that upon the exposure of the Nasr Institute as a front for Iranian state-sponsored offensive cyber activity, employees transitioned over to other entities, such as Kavosh, to protect their identities and minimize further exposure. There were no further widely reported exposures relating to the Nasr Institute until the links between Mahdi Honarvar to Kavosh Security Center were revealed in 2017. Therefore, we assess that the overlapping technical and personal information points to a historic linkage between the threat actors APT33, APT35, and MUDDYWATER.

These technical and persona overlaps among Iranian threat actors are not unexpected given the tiered structure of Iranian state management of cyber operations. Within this structure, we assessed that managers are running multiple teams, some of which are associated with government organizations and others that are contracted private companies (such as [ITSec Team](#)).

Technical Analysis

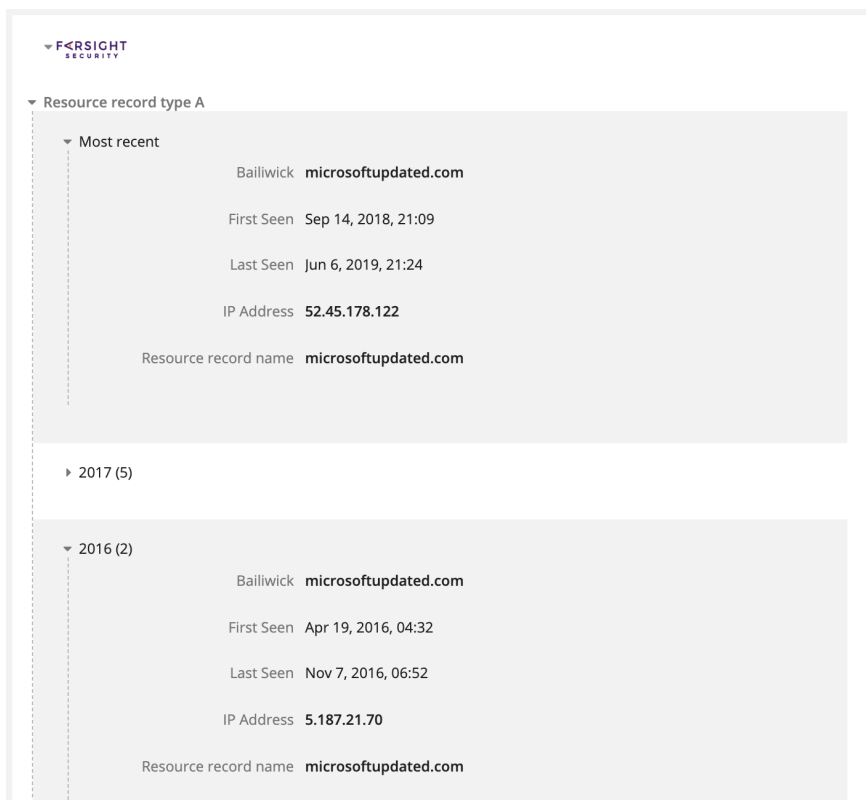
APT33 Cleaning Up?

Starting with the APT33 indicators documented by Symantec, Insikt Group profiled the domain and hosting infrastructure used by the group using the Farsight Security extension within the Recorded Future platform, revealing updated IP resolutions for some of the domains.

Domain	Original IP Resolution (Per Symantec Report)	Updated IP Resolutions
backupnet.ddns[.]net	5.187.21[.]71 91.230.121[.]143	95.183.54[.]119
hyperservice.ddns[.]net	8.26.21[.]119	95.183.54[.]119
microsoftupdated[.]com	5.187.21[.]70	52.45.178[.]122
mynetwork[.]cf	192.119.15[.]41 195.20.52[.]172	195.20.52[.]172
mynetwork.ddns[.]net	162.250.145[.]204 162.250.145[.]234 192.119.15[.]35 192.119.15[.]37 64.251.19[.]214 64.251.19[.]231 64.251.19[.]232 8.26.21[.]120 8.26.21[.]221 8.26.21[.]222	No Current Resolution
mypsh.ddns[.]net	5.79.127[.]177	0.0.0[.]0
mywinnetwork.ddns[.]net	91.235.142[.]76 91.235.142[.]124 89.34.237[.]118	0.0.0[.]0
remote-server.ddns[.]net	192.119.15[.]39 91.230.121[.]143	0.0.0[.]0
remserver.ddns[.]net	217.147.168[.]44 91.230.121[.]144	0.0.0[.]0
securityupdated[.]com	217.13.103[.]46	204.11.56[.]48
servhost.hopto[.]org	37.48.105[.]178	95.183.54[.]119 0.0.0[.]0
service-avant[.]com	213.252.244[.]14	213.252.244[.]144 51.77.102[.]108
srvhost.servehttp[.]com	8.26.21[.]117 64.251.19[.]216	95.183.54[.]119
svcexplores[.]com	188.165.4[.]81	-
update-sec[.]com	95.211.191[.]117	-

As expected, many of the domains exposed in the original Symantec report have been parked or no longer resolve to a real IPv4 address. Interestingly, four of the original domains (backupnet.ddns[.]net, hyperservice.ddns[.]net, servhost.hopto[.]org, and srvhost.servehttp[.]com) were all updated the day after publication, and resolve to the same IP, 95.183.54[.]119. This IP is registered to Swiss-dedicated hosting provider Solar Communications GmbH. It is unclear as to why these domains were not likewise parked. Possible reasons include:

- The domains were deemed high value by the threat actor, and therefore retained for continued operational purposes.
- The operators had difficulty with or could not update the domains for administrative reasons.



The screenshot shows a 'Resource record type A' entry for 'microsoftupdated.com'. It is categorized under 'Most recent' and includes the following details:

- Bailiwick: **microsoftupdated.com**
- First Seen: Sep 14, 2018, 21:09
- Last Seen: Jun 6, 2019, 21:24
- IP Address: **52.45.178.122**
- Resource record name: **microsoftupdated.com**

Below this, there are two other entries for the year 2016:

- 2017 (5)
- 2016 (2)
 - Bailiwick: **microsoftupdated.com**
 - First Seen: Apr 19, 2016, 04:32
 - Last Seen: Nov 7, 2016, 06:52
 - IP Address: **5.187.21.70**
 - Resource record name: **microsoftupdated.com**

Recorded Future Intelligence Card for microsoftupdated[.]com, enriched using the Farsight Security extension.

In order to identify additional related and potentially malicious infrastructure, we pivoted on the Swiss IP 95.183.54[.]119 and identified approximately 40 domains that were newly resolving to the IP since mid-February 2019. We positively identified RAT malware communication from a selection of domains.

Domain	IP	Malware Observed Communicating With Domain
windowsx.sytes[.]net	95.183.54[.]119	Nanocore
hellocookies.ddns[.]net	95.183.54[.]119	Nanocore QuasarRAT variant
njrat12.ddns[.]net	95.183.54[.]119	njRAT
trojan1117.hopto[.]org	95.183.54[.]119	njRAT
wwwgooglecom.sytes[.]net	95.183.54[.]119	njRAT
newhost.hopto[.]org	95.183.54[.]119	njRAT DarkComet
za158155.ddns[.]net	95.183.54[.]119	njRAT

Additionally, many of the domains that resolved to the Swiss IP were registered with hostnames that reflected the names of commodity RATs, such as XTreme RAT, xtreme.hopto[.]org, and njRAT (njrat12.ddns[.]net), as well as popular tools like Netcat (n3tc4t.hopto[.]com). Interestingly, a domain spoofing a popular Farsi-language Telegram channel called [BistBots](#) (bistbotsproxies.ddns[.]net) was also co-hosted on the same IP. We assess that this likely indicates a desire to target users of BistBots who seek up-to-date, high-speed internet proxies, possibly to circumvent network filtering and [access sites such as Facebook, Twitter, and YouTube](#), which are restricted in Iran.

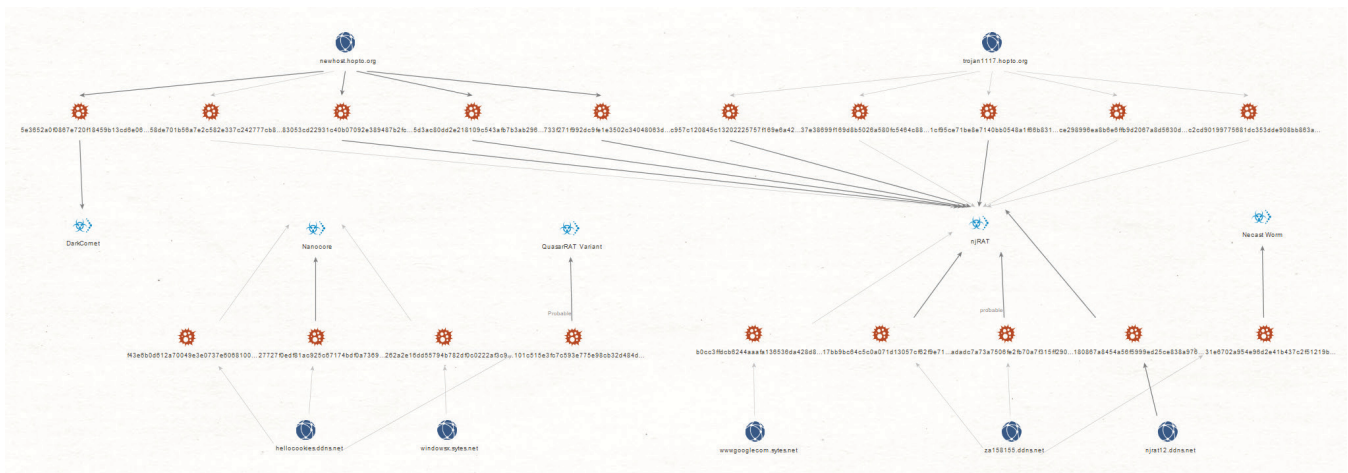
Further analysis of the domains above, including windowsx.sytes[.]net, njrat12.ddns[.]net, and wwwgooglecom.sytes[.]net shows that they have been classified as C2s for Nanocore and njRAT, according to their respective Recorded Future Intelligence Cards. The information detailed are correlations derived from hash reports from malware multiscanner repositories and malware detonations that contain direct references to the domains.

Interestingly, while the Symantec research noted APT33’s use of Nanocore, njRAT was not mentioned, which indicates a previously unknown addition to the group’s ever-expanding repertoire of commodity malware.

Context		
Malware Category	Hash 6 of 21	IP Address
Remote Access Trojan 5	505e84f4a38b0925284f53e46d7... 3 ● 70	8.8.4.4 1 ● 0
Trojan 4	6c770ea29bcf7701d6264b2074e... 3 ● 70	8.8.8.8 1 ● 0
Backdoor 1	10d8d1d5d34a6d375fe241ef289... 1 ● 0	Show in Table v
Show in Table v	1d31d9f784e3bf375dc97a95c075... 1 ● 0	
	3beadf2cf64cbd321f31a554775f7... 1 ● 0	Product
Domain	3c3ca31967eeafa13577804a46f4... 1 ● 0	VirusTotal 4
windowsx.sytes.net 1 ● 10	Show in Table v	ClamAV 1
Show in Table v		Win32 1
	Malware	AhnLab-V3 1
	Nanocore Remote Access Trojan 5	Show in Table v
	Show in Table v	
Show all entities in Table v		

Context panel from the Recorded Future Intelligence Card for windowsx.sytes[.]net, showing the relationship between the domain and the Nanocore RAT malware.

The Maltego chart below shows the link analysis of selected domains hosted on the Swiss IP, with derived hashes associated with malware family name.



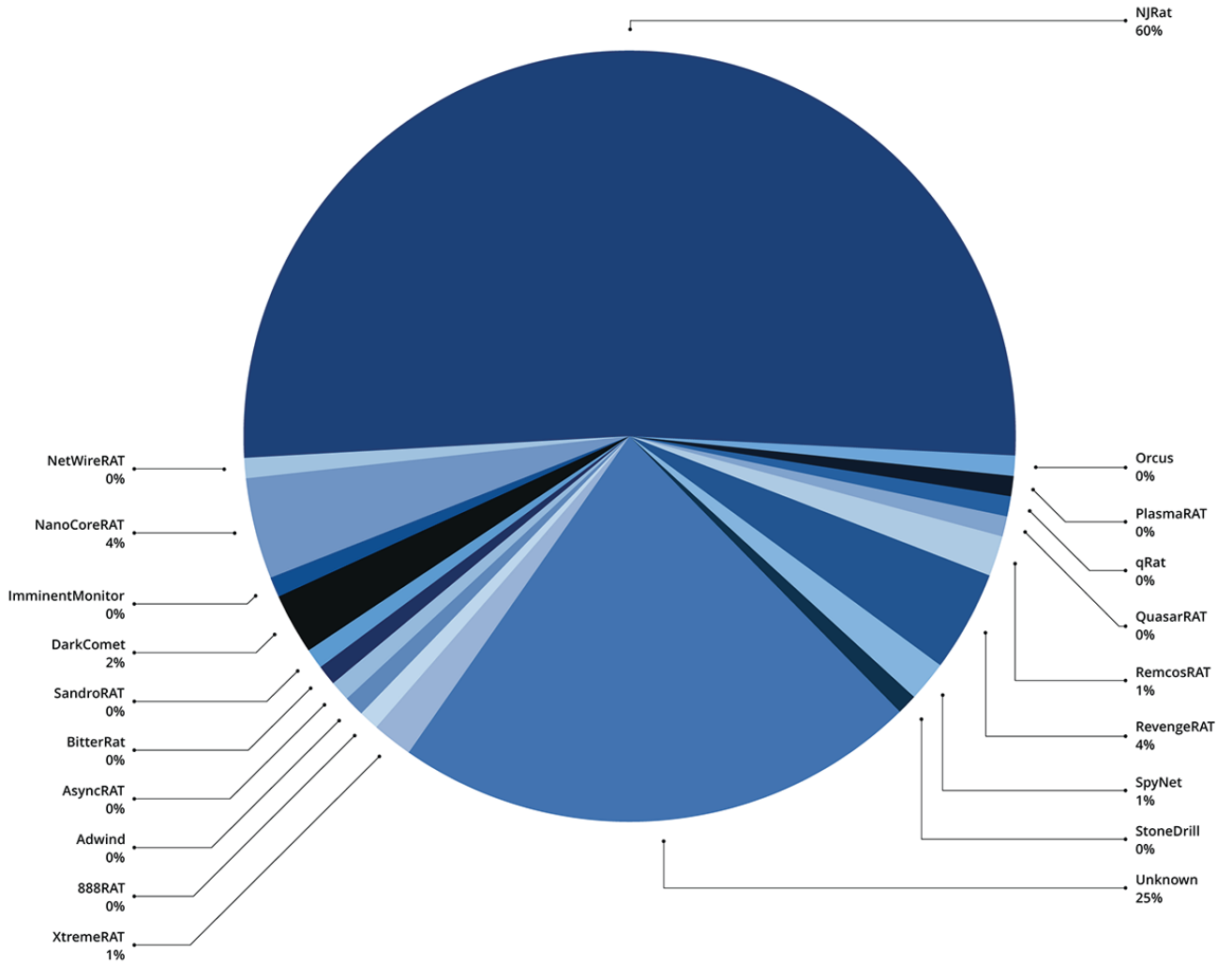
Maltego graph of domains hosted on the known malicious APT33-linked IP.

Deeper Infrastructure Correlations

Insikt Group enumerated all domains reported as being used by APT33 since January 2019. We pivoted through common infrastructure hosting patterns using passive DNS and similar approaches to identify additional suspected APT33 infrastructure.

A preliminary analysis identified 1,252 unique, correlated domains likely administered by the same APT33 attackers behind the campaign documented by Symantec. Of these, 728 domains were identified as communicating with files on infected hosts, with 575 of these positively correlated to a RAT malware family. The remaining 153 domains were identified as malicious based on AV engine hits but could not be conclusively classified to a specific malware family automatically.

***Editor's Note:** A selection of the domains, hashes, and associated IP address infrastructure connected to suspected APT33 domains will soon be made available to Recorded Future clients in a specialized Certified Data Set called "Weaponized Domains," enabling companies to regulate the interaction with malicious free/anonymous infrastructure, including dynamic DNS (DDNS) domains.*



SUSPECTED APT33 MALWARE USE
March 28 - June 6, 2019

Pie chart of suspected APT33 malware use.

A top-level activity breakdown of these suspected APT33 domains and their linked malware families since March 28, 2019 reveals that 60% of the domains use the njRAT malware, with a wide selection of other commodity tools being used. In total, 1,804 unique malware hashes were analyzed to classify them into the 19 malware families, listed below.

Malware Family	Percentage (%)
NjRat	59.99
unknown	25.35
RevengeRAT	4.40
NanoCoreRAT	3.96
DarkComet	1.74
SpyNet	0.87
RemcosRAT	0.76
XtremeRAT	0.60
ImminentMonitor	0.43
NetWireRAT	0.33
Orcus	0.33
QuasarRAT	0.27
888RAT	0.22
qRat	0.22
Adwind	0.16
SandroRAT	0.11
PlasmaRAT	0.11
AsyncRAT	0.05
BitterRat	0.05
StoneDrill	0.05

From the table and the accompanying chart, we noted that APT33, or a closely aligned threat actor, have been prolific in their continued use of commodity malware and publicly available tooling, and have added several malware families previously unreported to be associated with the threat actor, including njRAT, RevengeRAT, and AdwindRAT. A significant proportion of the samples (25%), while deemed malicious, contained generic code that could not be definitively classified at a high enough degree of confidence to warrant further manual static analysis. We will continue to focus closely on these samples in subsequent analyses.

Many of the domains uncovered spoofed global technology providers such as Microsoft and Google, as well as business-oriented, web-based services such as video conferencing provider Zoom. Geopolitically themed domains were also present in this list of suspected APT33 infrastructure, such as vichtorio-israeli.zapto[.]org (Victory to Israel), fucksaudi.ddns[.]com and palestine.loginto[.]me. The choice of hostnames may offer insight into the targeting pattern of APT33 operations against the Islamic Republic of Iran's perceived enemies — notably, Israel, Saudi Arabia, and the wider [Gulf Cooperation Council](#) (GCC) nations.

Domain	Malware Family	SHA256
fucksaudi.ddns[.]net	RevengeRAT	d8e60135aecb3a2a7422c06cfb94ed9aaf-1182145d1c482f84b0bd81aa5d2416
googlechromehost.ddns[.]net	NanoCoreRAT	e2cfc91085b9b5db41c4c4297c594758dd9a0c-8561ce4544da9faedd3a6b91e8
backupnet.ddns[.]net	StoneDrill	a217eb149b65552e3127c65c306aa521dca-54959ceee89e85dd2e6e38c0d8f8b
younesadams.ddns[.]net	SandroRAT	410b5f374059cc21b2c738a-71957c97e4183d92580d1d48df-887deece6d2f663
teamnj.ddns[.]net	DarkComet	e144db21cc5f8f57aa748c0a8e4008fc34f8d-d831eb2442eb35961e4cdf41f22

Selection of hashes correlated with suspected APT33 malicious domains. Recorded Future clients will be able to access the full list of domains in the Certified Data Set via API download.

Targeted Organizations

Using data from Recorded Future Domain Analysis and combining it with data derived from Recorded Future Network Traffic Analysis, Insikt Group researchers were able to identify a small selection of likely targeted organizations impacted by suspected APT33 activity.

Targeted Organization	Sector(s)	Country of Operation	Date of Observed Activity	Suspected APT33 C2 IP
Organization 1	Engineering & Construction, Water & Electricity, Technology, Retail Finance	Saudi Arabia UAE Egypt Turkey Croatia	May 2 - June 3, 2019	134.3.20[.]151
Organization 2	Mass Media	India	May 4 - June 1, 2019	134.3.20[.]151
Organization 3	Diplomatic	Burkina Faso	May 2, 2019	134.3.20[.]151
Organizations 4 and 5	Healthcare	Saudi Arabia	May 2 - May 8, 2019	41.103.3[.]7 46.249.47[.]193
Organization 6	Industrial	Saudi Arabia	May 25 - June 3, 2019	62.113.171[.]186

Outlook

Following the exposure of a wide range of their infrastructure and operations by Symantec earlier this year, we discovered that APT33, or closely aligned actors, reacted by either parking or reassigning some of their domain infrastructure. The fact that this activity was executed just a day or so after the report went live suggests the Iranian threat actors are acutely aware of the media coverage of their activities and are resourceful enough to be able to react in a quick manner.

Since late March, suspected APT33 threat actors have continued to use a large swath of operational infrastructure, well in excess of 1,200 domains, with many observed communicating with 19 different commodity RAT implants. An interesting development appears to be their increased preference for njRAT, with over half of the observed suspected APT33 infrastructure being linked to njRAT deployment.

While we haven't observed a widespread targeting of commercial entities or regional adversaries like in previously documented APT33 operations, the handful of targeted organizations that we did observe were mainly located in Saudi Arabia across a range of industries, indicating ongoing targeting aligned with geopolitical aims. We assess that the large amount of infrastructure uncovered in our research is likely indicative of wider ongoing operational activity, or the laying of groundwork for future cyberespionage operations. We recommend organizations take measures to monitor their networks for evidence of suspected APT33 activity by following the guidance in the "Network Defense Recommendations" section below.

Finally, our recommendation to Recorded Future clients is to use our upcoming "Weaponized Domains" Certified Data Set, which has been derived from predictive analytics that assist in the identification of malicious APT infrastructure. This is meant to empower your security teams to hunt, detect, and block high-fidelity malicious indicators at scale.

Network Defense Recommendations

Recorded Future recommends that organizations conduct the following measures in order to detect and mitigate suspected APT33 activity:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in Appendix A.
- As detailed in our previous blog on APT33 available to our clients only, Dynamic DNS (DDNS) continues to be a relevant operational choke point for security control implementation. All TCP/UDP network traffic involving DDNS subdomains should be blocked and logged (using [DNS RPZ](#) or similar).
- Conduct regular Yara scans across your enterprise for the new rules listed in Appendix B.

Appendix A — [Indicators of Compromise](#)

```
RevengeRAT - fucksaudi.ddns[.]net
d8e60135aecb3a2a7422c06cfb94ed9aaf1182145d1c482f84b0bd81aa5d2416
NanoCoreRAT - googlechromehost.ddns[.]net
e2cfc91085b9b5db41c4c4297c594758dd9a0c8561ce4544da9faedd3a6b91e8
StoneDrill - backupnet.ddns[.]net
a217eb149b65552e3127c65c306aa521dca54959ceee89e85dd2e6e38c0d8f8b
SandroRAT - younesadams.ddns[.]net
410b5f374059cc21b2c738a71957c97e4183d92580d1d48df887deece6d2f663
DarkComet - teamnj.ddns[.]net
e144db21cc5f8f57aa748c0a8e4008fc34f8dd831eb2442eb35961e4cdf41f22
bistbotsproxies.ddns[.]net
hellocookies.ddns[.]net
hyperservice.ddns[.]net
microsoftupdated[.]com
mynetwork.ddns[.]net
mynetwork[.]cf
mypsh.ddns[.]net
mywinnetwork.ddns[.]net
n3tc4t.hopto[.]com
newhost.hopto[.]org
njrat12.ddns[.]net
remote-server.ddns[.]net
remserver.ddns[.]net
securityupdated[.]com
servhost.hopto[.]org
service-avant[.]com
srvhost.servehttp[.]com
svcxplores[.]com
trojan1117.hopto[.]org
update-sec[.]com
windowsx.sytes[.]net
wwwgooglecom.sytes[.]net
xtreme.hopto[.]org
za158155.ddns[.]net

134.3.20[.]151
188.165.4[.]81
195.20.52[.]172
204.11.56[.]48
213.252.244[.]144
41.103.3[.]7
46.249.47[.]193
51.77.102[.]108
52.45.178[.]122
62.113.171[.]186
95.183.54[.]119
95.211.191[.]117
```

Appendix B — [Yara Rules](#)

Please refer to linked file.

Appendix D — MITRE Pre-ATT&CK Mapping

MITRE PRE-ATT&CK Mapping

Priority Definition Planning	Priority Definition Direction	Technical Information Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary Opsec	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilities
Assess Current Holdings, Needs And Wants	Assign KTs, NQs, AND/OR Intelligence Requirements	Determine Approach/Attack Vector	Acquire OSINT Data Sets And Information	Acquire OSINT Data Sets And Information	Acquire OSINT Data Sets And Information	Analyze Application Security Posture	Analyze Organizational Skills And Deficiencies	Analyze Business Processes	Acquire And/Or Use 3rd Party Infrastructure Services	Build Social Network Persona	Build And Configure Delivery Systems	Review Logs And Residual Traces	Disseminate Removable Media	
Access KTX/Kqs Benefits	Receive KTs/Kqs And Determine Requirements	Determine Highest Level Tactical Element	Conduct Active Scanning	Aggregate Individual's Digital Footprint	Conduct Social Engineering	Analyze Architecture And Configuration Posture	Analyze Social And Business Relationships, Interests, And Affiliations	Analyze Organizational Skills And Deficiencies	Acquire And/Or Use 3rd Party Software Services	Acquire And/Or Use 3rd Party Software Services	Choose Precompromised Mobile App Developer Account Credentials Or Signing Keys	Build Or Acquire Exploits	Test Ability To Evade Automated Mobile Application Security Analysis Performed By App Stores	Distribute Malicious Software Development Tools
Assess Leadership Areas Of Interest	Submit KTs, NQs, And Intelligence Requirements	Determine Operational Element	Conduct Passive Scanning	Conduct Social Engineering	Determine 3rd Party Infrastructure Services	Analyze Data Collected	Assess Targeting Options	Analyze Presence Of Outsourced Capabilities	Acquire Or Compromise 3rd Party Signing Certificates	Acquire Or Compromise 3rd Party Signed Certificates	Choose Precompromised Persona And Affiliated Accounts	C2 Protocol Development	Test Callback Functionality	Friend/Follow/Connect To Targets Of Interest
Assign KTX/Kqs Into Categories	Task Requirements	Determine Secondary Level Tactical Element	Conduct Social Engineering	Identify Business Relationships	Determine Certification Of IT Management	Analyze Hardware/Software Security Defensive Capabilities		Assess Opportunities Created By Business Deals	Anonymous Services	Buy Domain Name	Develop Social Network Persona Digital Footprint	Compromise 3rd Party Or Closed-Source Vulnerability Exploit Information	Test Malware In Various Execution Environments	Hardware Or Software Supply Chain Implant
Conduct Cost/Benefit Analysis		Determine Strategic Target	Determine 3rd Party Infrastructure Services	Identify Groups/Roles	Determine Physical Locations	Analyze Organizational Skills And Deficiencies		Assess Security Posture Of Physical Locations	Common, High Volume Protocols And Software	Compromise 3rd Party Infrastructure To Support Delivery	Friend/Follow/Connect To Targets Of Interest	Create Custom Payloads	Test Malware To Evade Detection	Port Redirection
Create Implementation Plan			Determine Domain And IP Address Space	Identify Job Postings And Needs/Gaps	Dumpster Dive	Identify Vulnerabilities In Tertiary Software Libraries		Assess Vulnerability Of 3rd Party Vendors	Compromise 3rd Party Infrastructure To Support Delivery	Create Backup Infrastructure	Obtain Aggie IDS Enterprise Distribution Key Pair And Certificate	Create Infected Removable Media	Test Physical Access	Upload, Install, And Configure Software/Tools
Create Strategic Plan			Determine External Network Trust Dependencies	Identify People Of Interest	Identify Business Processes/Tempo	Research Relevant Vulnerabilities/ CVEs		Data Hiding	Domain Registration Hijacking	Dynamic DNS	Discover New Exploits And Monitor Exploit-Provider Forums	Identify Resources Required To Build Capabilities	Test Signature Detection For File Upload/Email Filters	
Derive Intelligence Requirements			Determine Firmware Version	Identify Personnel With An Authority/Privilege	Identify Business Relationships	Research Visibility Gap Of Security Vendors		Dynamic DNS	Dynamic DNS	Dynamic DNS	Obtain Re-Use Payloads	Post-Compromise Tool Development		
Develop KTX/NQs			Discover Target Login/Email Address Format	Identify Sensitive Personnel Information	Identify Job Postings And Needs/Gaps	Test Signature Detection		Dynamic DNS	Obfuscate Infrastructure	Obfuscate Infrastructure	Remote Access Tool Development			
Generate Analyst Intelligence Requirement			Enumerate Client Configurations	Identify Supply Chains	Identify Supply Chains			Fast Flux DNS	Obtain Booster/Stressor Subscription	Obtain Booster/Stressor Subscription				
Identify Analyst Level Gaps			Enumerate Externally Facing Software Applications, Technologies, Languages, And Dependencies	Mine Social Media	Obtain Templates/Branding Materials			Host-Based Hiding Techniques	Procure Required Equipment And Software	Procure Required Equipment And Software				
Identify Gap Areas			Identify Job Postings And Needs/Gaps					Misattributable Credentials	Shadow DNS	Shadow DNS				
Receive Operator KTX/Kqs Tasking			Identify Security Defensive Capabilities					Network-Based Hiding Techniques	SSL Certificate Acquisition For Domain	SSL Certificate Acquisition For Domain				
			Identify Supply Chains					Non-Traditional Or Less Attributable Payment Options	SSL Certificate Acquisition For Trust Breaking	SSL Certificate Acquisition For Trust Breaking				
			Identify Technology Usage Patterns					Obfuscate Infrastructure	Use Multiple DNS Infrastructures	Use Multiple DNS Infrastructures				
			Identify Web Defensive Services					Obfuscate Operational Infrastructure						
			Map Network Topology					Obfuscate Or Encrypt Code						
			Mine Technical Blog/Forums					Obfuscation Or Cryptography						
			Obtain DomainIP Registration Information Spearphishing For Information					OS-Vendor Provided Communication Channels						
								Private-Wholesale Services						
								Proxy/Protocol Relays						
								Secure And Protect Infrastructure						

LEGEND
 ● PRE-ATT&CK mapping for suspected APT33 activity March

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.