The Record.
Recorded Future® News

IMAGE: ELIF ÖZLEM AYDENIZ VIA PEXELS

Daryna Antoniuk

December 15th, 2023

Nation-state Briefs Malware

Get more insights with the
Recorded Future
Intelligence Cloud.

Learn more.

Iran-linked hackers develop new malware downloaders to infect victims in Israel

A cyber-espionage group linked to the Iranian government developed several new malware downloaders over the past two years and has recently been using them to target organizations in Israel.

Researchers at the Slovakia-based company ESET attributed the newly discovered downloaders to the Iranian advanced persistent threat group OilRig, also known as APT34.

Previous reports said the group primarily targeted organizations in the Middle East this year, especially focusing on Israel during its ongoing war with the Palestinian militant group Hamas.

ESET researchers labeled the three new malware downloaders as ODAgent, OilCheck and OilBooster. The hackers also released an updated version of their previous downloader, dubbed SampleCheck5000.

All of them were deployed against Israeli targets, including those in the healthcare sector, a manufacturing company and a local governmental organization, all of which had previously been affected by multiple OilRig tools.

“It underlines the fact that OilRig is persistent in targeting the same organizations, and determined to keep its foothold in compromised networks,” researchers said.

OilRig also is trying to hide its activity by using well-known cloud service providers for command-and-control communication, ESET said.

This strategy allows the malicious downloaders to blend their activity more easily into the regular stream of network traffic, the researchers said. OilRig typically uses the malware to send in other malicious software and exfiltrate files.

The researchers couldn’t identify the initial attack vector used by hackers to compromise Israeli networks. They also couldn’t confirm whether the attackers have been able to successfully compromise the same organizations repeatedly or if they somehow managed to maintain their foothold in the network between deploying various tools.

However, “the continuous development and testing of new variants, experimentation with various cloud services and different programming languages, and the dedication to re-compromise the same targets over and over again, make OilRig a group to watch out for,” says ESET researcher Zuzana Hromcová, in a statement shared with Recorded Future News.

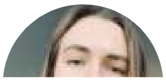
Tags

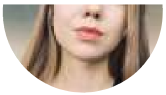
Israel Iran OilRig APT34

Previous article Next article

← →

DARYNA ANTONIUK





Daryna Antoniuk is a freelance reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.

BRIEFS

UK privacy watchdog to examine practice of web scraping to get training data for AI

| January 15th, 2024

Microsoft to keep all European cloud customers' personal data within EU

| January 13th, 2024

British cosmetics firm Lush confirms cyberattack| January 13th, 2024

FCC presses carmakers, wireless providers to protect domestic abuse survivors from stalking tools

| January 12th, 2024

Further analysis of Denmark attacks leads to warning about unpatched network gear

| January 12th, 2024

Republican lawmakers want answers on SEC social media hack — and soon

| January 11th, 2024

French hacker from 'ShinyHunters' group sentenced to three years in US prison

| January 11th, 2024

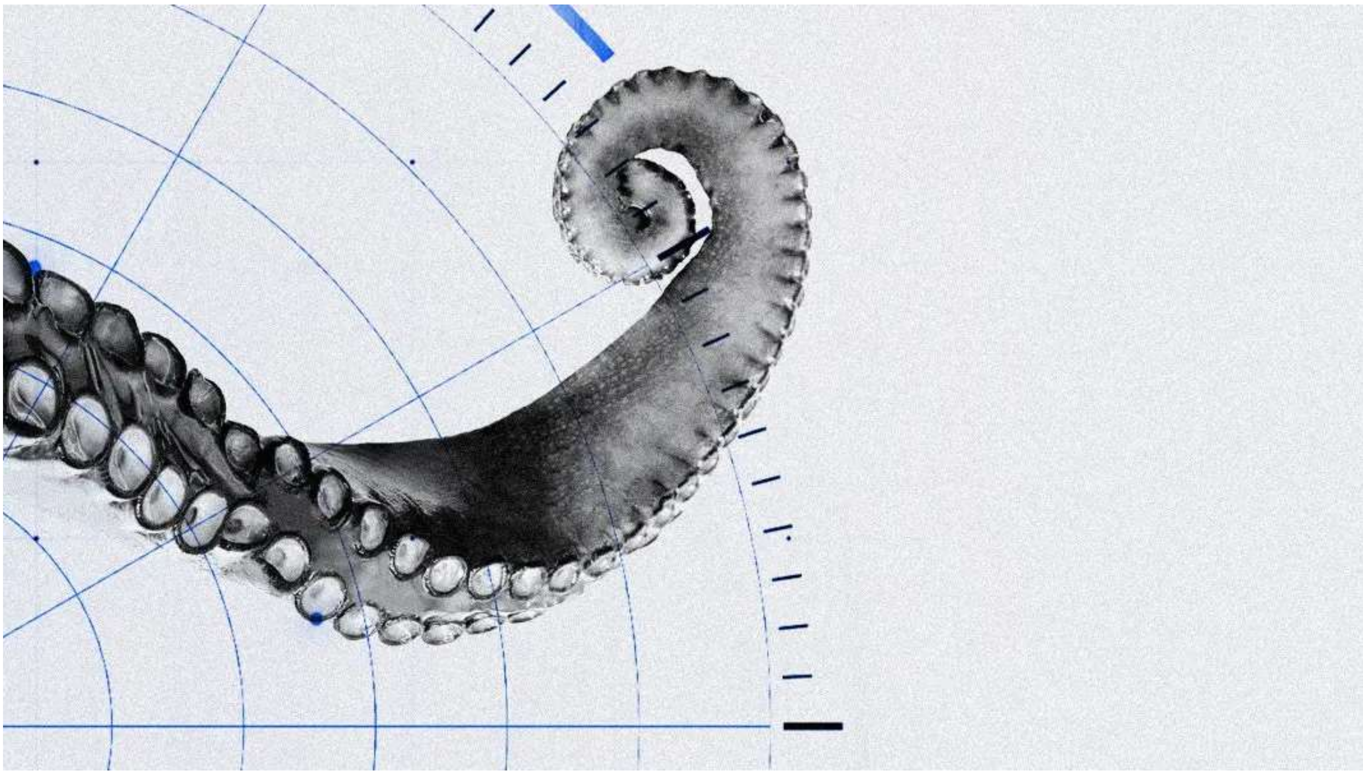
SEC's X account compromised, used to spread false bitcoin announcement

| January 10th, 2024

Nigerian national who laundered funds from romance and BEC scams gets 10-year sentence

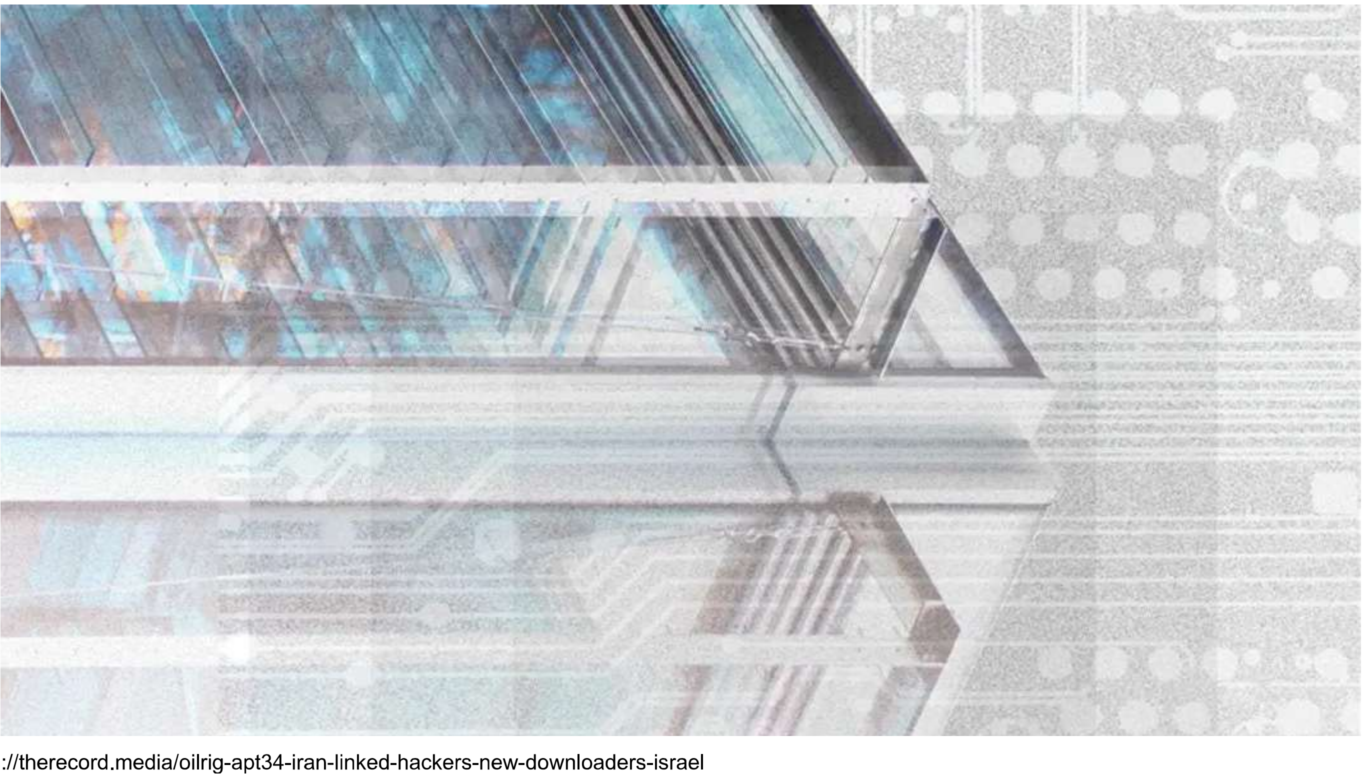
| January 10th, 2024

FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE



FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE

2023 ADVERSARY INFRASTRUCTURE REPORT



2023 ADVERSARY INFRASTRUCTURE REPORT

ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK “DOPPELGÄNGER” SIGNALS EVOLVING TACTICS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK “DOPPELGÄNGER” SIGNALS EVOLVING TACTICS

The Record.
Recorded Future® News

Privacy About Contact Us

© Copyright 2024 | The Record from Recorded Future News