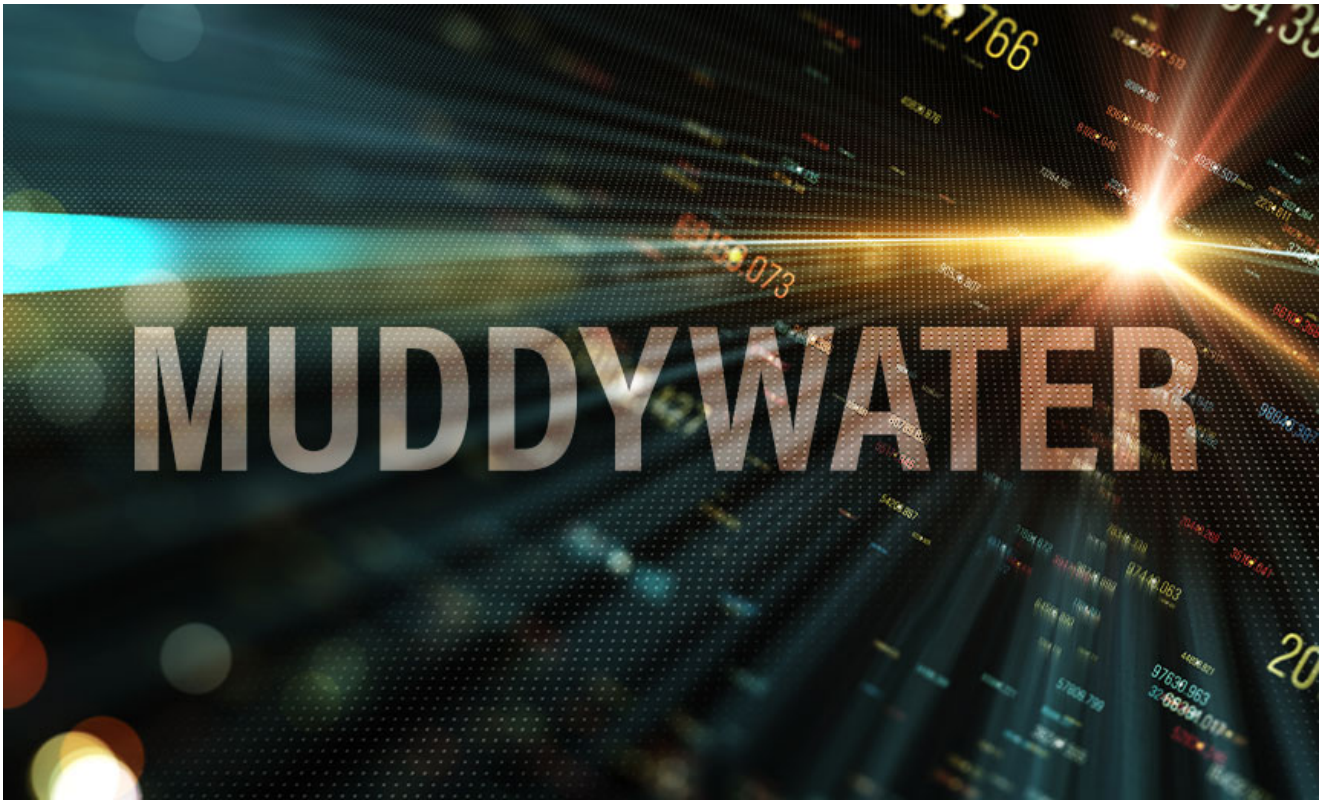
MuddyWater Targets Critical Infrastructure in Asia, Europe

inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611

Application Security , Cybercrime , Cybercrime as-a-service

Iran-Backed Hacking Group Targets Telecom, Defense, Government Sectors Prajeet Nair (@prajeetspeaks) • February 25, 2022



MuddyWater is expected to exploit the world's focus on Ukraine.

Hacking group MuddyWater, which has been linked to the Iranian Ministry of Intelligence and Security is targeting government and private sector organizations in Asia, Africa, Europe and North America as part of its cyberespionage and other malicious cyber operations, according to a joint advisory from U.S. and U.K. law enforcement and intelligence agencies.

See Also: OnDemand | Understanding Human Behavior: Tackling Retail's ATO & Fraud Prevention Challenge

Sectors targeted by the advanced persistent threat actor include telecommunications, defense, local government, and oil and natural gas. The advisory details the tactics, techniques and procedures, as well as the indicators of compromise, associated with the threat group.

Dirk Schrader, resident CISO, EMEA, and vice president of security research at cybersecurity firm Netwrix, says government-linked APTs such as MuddyWater will use the Russia-Ukraine conflict for their own purposes. Knowing that focus and attention are directed there, he says, the groups may use adapted spear-phishing emails while everyone is expecting a massive cyber operation.

MuddyWater was earlier suspected of using ransomware to damage the systems of organizations in Israel and other countries. The group is also known as EMP.Zagros, Static Kitten, Mercury and Seedworm (see: *Iranian Hacking Group Suspected of Deploying Ransomware*).

About MuddyWater

MuddyWater, a subordinate element in the Iranian Ministry of Intelligence and Security, has conducted broad cyber campaigns in support of MOIS objectives since 2018, the advisory says.

In 2017 Kaspersky spotted MuddyWater using spear-phishing techniques to target government agencies, military institutions, telecommunications companies and universities throughout the Middle East.

The threat group is positioned to provide the Iranian government with stolen data and access to systems and to share these with other malicious cyber actors, the advisory says, citing analysis by the U.K National Cyber Security Center, the U.S. Cybersecurity and Infrastructure Security Agency, the National Security Agency, the Federal Bureau of Investigation and U.S. Cyber Command's Cyber National Mission Force.

The Iranian government-sponsored group was exploiting publicly known vulnerabilities and leveraging multiple open-source tools to gain access to sensitive government and commercial networks and deploy ransomware, the advisory says. "These actors also maintain persistence on victim networks via tactics such as side-loading dynamic link libraries, to trick legitimate programs into running malware and obfuscating PowerShell scripts to hide command and control functions."

Technical Analysis

"MuddyWater attempts to coax their targeted victim into downloading ZIP files, containing either an Excel file with a malicious macro that communicates with the actor’s command and control server or a PDF file that drops a malicious file to the victim’s network," the advisory says.

It also uses multiple malware sets, such as PowGoop, Small Sieve, Canopy/Starwhale, Mori and POWERSTATS for loading malware, backdoor access, persistence and exfiltration.

"APT groups will rearrange their TTPs after being called out. That reinforces the need to be prepared, to have an established security architecture, with embedded workflows that dissolve security silos often seen in organizations, where protecting infrastructure, identities and data is handled in different ways, while attackers will use holes in all three layers to achieve their objectives," Netwrix's Schrader tells Information Security Media Group.

PowGoop

The campaign appears to be using a malicious loader named PowGoop - a fake Google Update mechanism - consisting of a DLL loader and a PowerShell-based downloader.

The malicious file impersonates a legitimate file that is signed as a Google Update executable file. The PowGoop samples analyzed by CISA and CNMF shows it has components to retrieve encrypted commands from a C2 server.

Small Sieve
A sample analyzed by the NCSC determined Small Sieve to be a Python backdoor distributed using a Nullsoft Scriptable Install System installer, gram_app.exe, which installs the Python backdoor, indoor.exe, and adds it as a registry run key that enables persistence.

"MuddyWater disguises malicious executables, and uses filenames and registry key names associated with Microsoft's Windows Defender to avoid detection during a casual inspection. The APT group has also used variations of Microsoft (e.g., 'Microsift') and Outlook in its filenames associated with Small Sieve," the advisory says.

The backdoor provides the basic functionality required to maintain and expand a foothold in the victim's infrastructure and avoid detection by using custom string and traffic obfuscation schemes together with the Telegram Bot application programming interface, the advisory says. It says the Small Sieve's beacons and tasking are performed using Telegram API.

Canopy

Canopy or Starwhale malware is another sample that MuddyWater distributes using spear-phishing emails with targeted attachments. In samples analyzed by CISA, a malicious Excel file, Cooperation terms.xls, contained macros written in Visual Basic for Applications and two encoded Windows Script Files. When the victim opens the Excel file, they receive a prompt to enable macros. Once this occurs, the macros are executed, decoding and installing the two embedded Windows Script Files.

Mori

The advisory says that the APT group MuddyWater also uses the Mori backdoor, which uses Domain Name System tunneling to communicate with the group’s C2 infrastructure.

"According to one sample analyzed by CISA, FML.dll, Mori uses a DLL written in C++ that is executed with regsvr32.exe with export DllRegisterServer, which appears to be a component to another program," the advisory says.

Some of the tasks performed include deleting the file FILENAME.old and deleting the file by registry value, it says.

POWERSTATS

The APT group is also known to use the POWERSTATS backdoor, which runs PowerShell scripts to maintain persistent access to the victim systems.

"CNMF has posted samples further detailing the different parts of MuddyWater's new suite of tools - along with JavaScript files used to establish connections back to malicious infrastructure - to the malware aggregation tool and repository, Virus Total," the advisory says.

The government agencies recently observed MuddyWater exploiting the Microsoft Netlogon elevation of privilege vulnerability CVE-2020-1472 and the Microsoft Exchange memory corruption vulnerability CVE-2020-0688.

Mitigation

Organizations must proactively maintain reasonable cyber hygiene aligned with business context, says Yaniv Bar-Dayan, CEO and co-founder of cyber risk remediation provider Vulcan Cyber.

"IT security teams must first ask themselves: 'What are the crown jewels of my organization?' and then work to secure these priorities. An orchestrated and deliberate approach to risk measurement, management and mitigation will deliver the needed security to protect against the hacker group flavor of the day," Bar-Dayan says.

The joint advisory also recommends deploying application control software to limit the applications and executable code that can be run by users. Email attachments and files downloaded via links in emails often contain executable code.