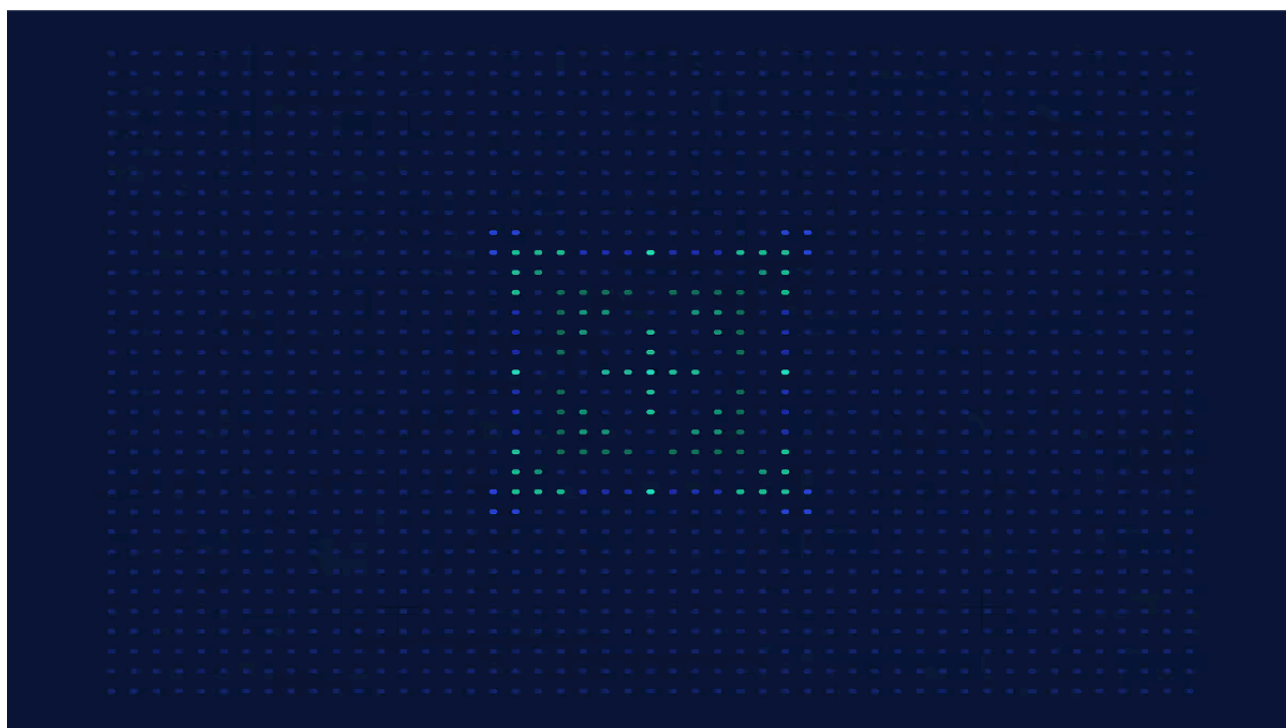
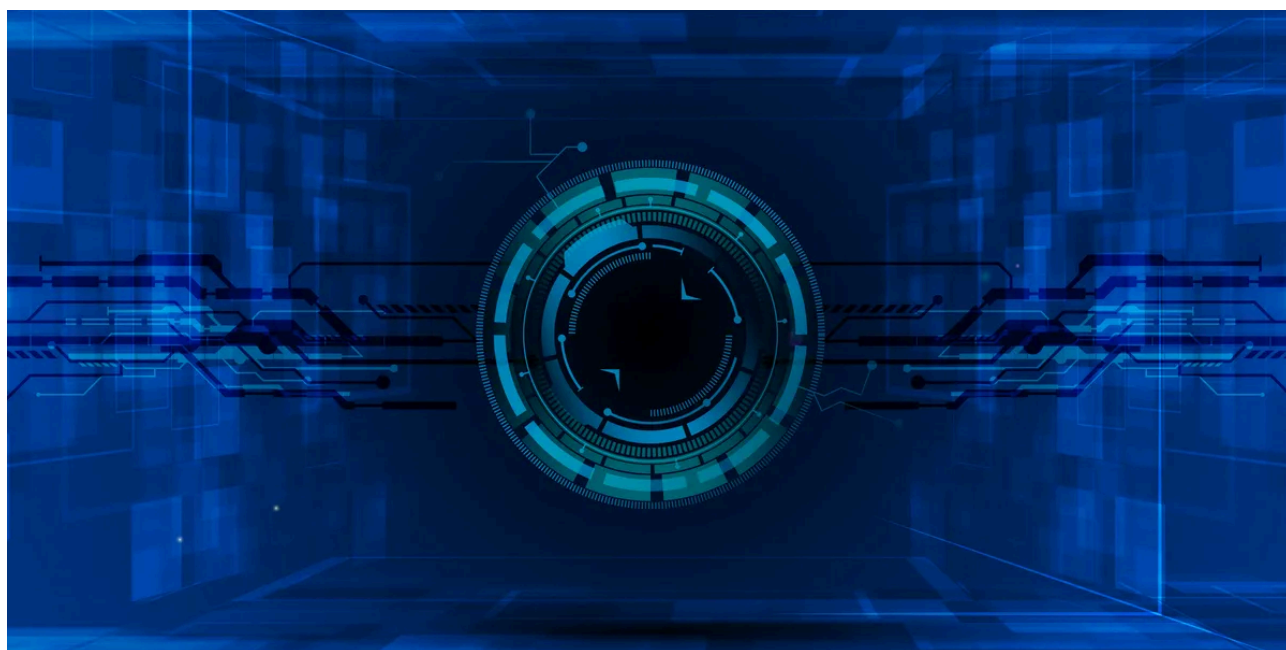


Evasive Maneuvers by the Wekby Group with Custom ROP-packing and DNS Covert Channels

By Aaron Shelmire

Published: 2026-03-12 · Archived: 2026-04-05 17:32:23 UTC

Evasive maneuvers by Wekby (TG-0416) from 30 Jun 2015: obfuscated HTTPBrowser/Token Control using DNS covert channels, custom ROP-packing, and IT-helpdesk phishing



ThreatStream Labs recently became aware of a campaign beginning on 30 June 2015 by the omnipresent Wekby threat actors (a/k/a [TG-0416](#), [APT-18](#), Dynamite Panda). The Wekby actors have recently been observed compromising organizations in the Manufacturing, Technology and Utilities verticals, but have had a long standing interest in the HealthCare industry. This campaign uses obfuscated variants of the HTTPBrowser tool that use DNS as a control channel.

This recent campaign exhibits many of the groups key characteristics to deliver a more technically advanced version of their toolkit than has previously been found. The Wekby group is keen on using phishes that purport to be from the IT helpdesk, often with links or attachments claiming to be vpn or citrix upgrades. This specific instance used a “cisco” vpnclient theme.

The Phishing links are:

hXXp://it-desktop[.]com/vpn/cisco/vpnclient.exe

hXXp://wangke99[.]tgk[.]delldns[.]com/tools.exe

These URIs result in the download of an installer, which creates a PE of the malware typically known as HTTPBrowser, but called Token Control by the Wekby group themselves (based upon the PDB strings found within many of the samples). The PEBuildDate of the installers range from 2015-06-30 11:57:13 to 12:03:13 UTC. Two samples use subdomains of local.it-desktop.com and were submitted to VirusTotal at 15:32:37 from users in Great Britain. At that time only 8 of 55 AntiVirus engines detected the same as malware, mostly with generic and heuristic detections. The third sample was first submitted on July 1st 2015 from a user in South Korea.

The samples install HTTPBrowser at *%APPDATA%/wdm.exe*. Persistence is established via the *HKCUSoftwareMicrosoftWindowsCurrentVersionRun* key value for *wdm* set to the path of the executable. Previous samples have set persistence via Run key values for *360v*.

HKCU Run Key for wdm

This tool has been used by a few groups since at least 2012 based upon PEBuildDates). However this sample is a bit more interesting. Normally HTTPBrowser sends traffic over HTTP using a user-agent of *HTTPBrowser/1.0*.

This sample uses DNS as a covert channel for communications. Specifically this sample utilizes DNS TXT records with 9 uppercase letters followed by a number and 7 more uppercase letters, then the C2 domain used. In this PCAP the C2 domain is glb.it-desktop.com. The “glb” label is believed to be a campaign ID. The other samples use the C2 domains of local.it-desktop.com and hi.getgo2.com

DNS TXT C2

Adding to the intrigue of this sample is a novel form of obfuscation that greatly complicates analysis. Specifically the sample uses Return Oriented Programming to control execution flow, and creates an extraordinary amount of functions filled with instructions that essentially evaluate to elaborate NOPs (no operation). The way this works is each function modifies the stack to replace the return point with additional functions including a function that includes the next bit of code that needs to be executed. Each subroutine includes the bare minimum number of operations necessary to call another subroutine, or perform local control flow (looping, branching, and simple

calculations), before modifying the stack to return to the next subroutine. While looking at a sample in OllyDbg, you would see the following, where execution will continue with Subroutine *0x0040F62E*. If that subroutine does not add any additional functions to the stack, execution will continue to Subroutine *0x0040F38A*.

ROP Obfuscation

While many of the Wekby threat actors campaigns may appear unsophisticated because they often rely upon stolen credentials or basic malware, this group of actors is extremely successful at obtaining their objectives. If your organization does not use Two-Factor authentication, the group will typically rely upon stolen credentials for remote access. The Wekby group has exhibited a preference to use a tool named HcdLoader which often persists as a Windows Service on externally facing servers for remote access. The group is particularly skilled at living off the land by using the tools already present on computers for [lateral movement](#) and exfiltration.

The samples detailed here can be found on VirusTotal at:

[d0f79de7bd194c1843e7411c473e4288](https://www.virustotal.com/file-d0f79de7bd194c1843e7411c473e4288/analysis/0)

[e5414c5215c9305feeebbe0dbee43567](https://www.virustotal.com/file-e5414c5215c9305feeebbe0dbee43567/analysis/0)

[985eba97e12c3e5bce9221631fb66d68](https://www.virustotal.com/file-985eba97e12c3e5bce9221631fb66d68/analysis/0)

UPDATE: The original post noted a domain of [hi.get2go.com](#) in error. This domain should have been [hi.getgo2.com](#)

Source: <https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop>