Hunting the hunter: BI.ZONE traces the footsteps of Red Wolf

By BI.ZONE

Published: 2023-06-28 · Archived: 2026-04-05 13:24:02 UTC

BI.ZONE Cyber Threat Intelligence team has detected a new campaign by Red Wolf, a hacker group that specializes in corporate espionage. Similar to its previous campaigns, the group continues to leverage phishing emails to gain access to the target organizations. To deliver malware on a compromised system, Red Wolf uses IMG files containing LNK files. By opening such a file an unsuspecting victim runs an obfuscated DLL file, which in its turn downloads and executes `RedCurl.FSABIN` on the victim's device. This enables the attackers to run commands in the compromised environment and transfer additional tools for post-exploitation.

Key findings

- Red Wolf continues to use traditional malware delivery methods, such as phishing emails that contain links to download malicious files
- In the campaign detected by BI.ZONE, the attackers used IMG files with malicious shortcuts to download and run `RedCurl.FSABIN`
- The group’s arsenal includes its own framework as well as a number of conventional tools, such as LaZagne and AD Explorer. To address its post-exploitation objectives, the group actively uses PowerShell
- Red Wolf focuses on corporate espionage and prefers to slowly move forward in the compromised IT infrastructure. By not drawing much attention, it can remain invisible for up to six months

Campaign

BI.ZONE Cyber Threat Intelligence team has unearthed a new campaign by the Red Wolf group (aka RedCurl) that has been active at least since June 2018 in Russia, Canada, Germany, Norway, Ukraine, and the United Kingdom.

The detected file (fig. 1) is an optical disk image. Once opened, it mounts onto the compromised system.

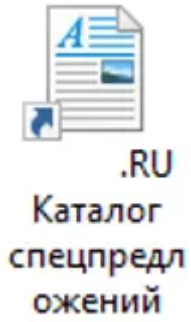

Fig. 1. Visible content of the disk image

The disk image contains an LNK file and a hidden folder `#TEMP` (fig. 2). The folder contains several DLL files, and only one of them has malicious content.

ekuvaMCE.dll	6/30/2022 6:26 AM	Application extens	105 KB
enCVsSmT.dll	6/23/2022 6:26 AM	Application extens	174 KB
IfFSeuWI.dll	7/13/2022 6:26 AM	Application extens	235 KB
ITxzUXVW.dll	9/7/2022 6:26 AM	Application extens	214 KB
kPLOVngW.dll	6/21/2022 6:26 AM	Application extens	174 KB
LsgbKZAa.dll	8/7/2022 6:26 AM	Application extens	214 KB
mKdPDaed.dll	9/17/2022 6:26 AM	Application extens	166 KB
peStwCWb.dll	8/28/2022 6:26 AM	Application extens	174 KB
qwAvfzNI.dll	9/4/2022 6:26 AM	Application extens	214 KB
roeEJpqS.dll	9/9/2022 6:26 AM	Application extens	174 KB
VjaLEtor.dll	6/22/2022 6:26 AM	Application extens	214 KB
vTepKaEk.dll	7/26/2022 6:26 AM	Application extens	174 KB
yTfjnFwL.dll	6/22/2022 6:26 AM	Application extens	214 KB

Fig. 2. Files in `#TEMP`

Opening the LNK file triggers the execution of `rundll32` with the following parameters:

```
rundll32.exe #temp\mKdPDaed.dll,ozCutPromo
```

The DLL file opens a web page (fig. 3).

Press enter or click to view image in full size

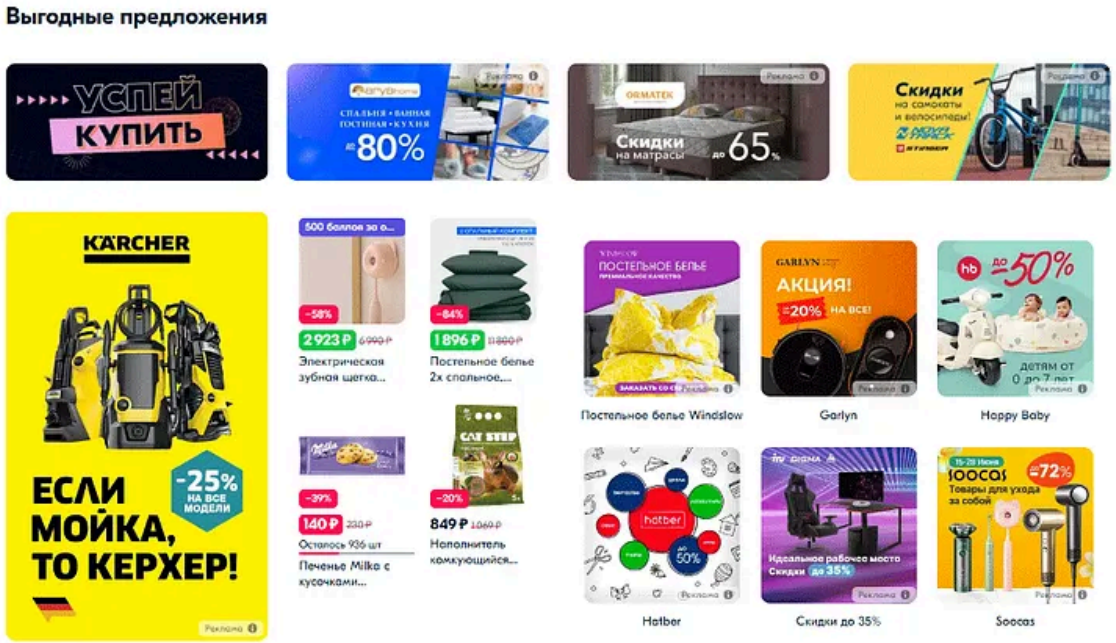

Fig. 3. Web page opened by the DLL file

After that, `RedCurl.FSABIN` gets downloaded from `https://app-ins-001.amscloudhost[.]com:443/dn01` and stored at `C:\Users\[user]\AppData\Local\VirtualStore\` under the name `chrminst_[computer name in base64].exe`. The strings in the file are encrypted with AES-128 CBC. The first part of the password for the key can be found directly in the malware sample, while the second one can be retrieved from the command line, for instance:


```
C:\Users\[redacted]\AppData\Local\VirtualStore\chrminst_[redacted].exe DOFBBdXC5DmPC
```

To achieve persistence in the compromised system, a task named `ChromeDefaultBrowser_Agent_[computer name in base64]` is created in the Windows Task Scheduler.

The backdoor uses Windows API to gather information on the number of processors, memory size, storage capacity, as well as information on the amount of time that passed since the launch of the operating system before the malware sample being launched. This checkup is needed to identify a virtual environment and bypass respective security and analysis tools. Once the checkup is completed, the backdoor sends information about the compromised system to the command-and-control server. This information includes the username, the computer name, the domain name, a list of files and folders in Program Files, Desktop, and AppData\Local, and the unique identifier. After that, the backdoor downloads the DLL and executes its exported function (in this case, `yDNvu`).

Conclusions

Despite the widely known attack techniques, Red Wolf still manages to bypass traditional defenses and minimize the likelihood of detection. By not drawing much attention, the group is able to remain unnoticed in the compromised infrastructure for a long time and achieve its goals.

How to detect the traces of Red Wolf

1. Monitor the creation and mounting of small disk image files
2. Pay attention to the DLL files run by rundll32 from `#TEMP`
3. Track suspicious files run by the Windows Task Scheduler from `C:\Users\[user]\AppData\Local`
4. Look for traces of network communications with subdomains `*.amscloudhost[.]com`
5. Prioritize the detection of tactics, techniques, and procedures specific to Red Wolf

MITRE ATT&CK

Press enter or click to view image in full size

Tactic	Technique	Procedure
Initial Access	Phishing: Spearphishing Link	Red Wolf uses phishing links in emails to deliver malware
Execution	User Execution: Malicious File	The victim needs to open the malicious LNK file to commence the compromise process
	Native API	Red Wolf employs Windows API to gather information about the compromised system
Defense Evasion	Hide Artifacts: Hidden Files and Directories	Red Wolf puts the malicious file in the hidden `#TEMP` folder
	System Binary Proxy Execution: Rundll32	Red Wolf uses `rundll32` to launch the malicious DLL
	Obfuscated Files or Information	Red Wolf uses `AES-128 CBC` to encrypt strings
	Virtualization/Sandbox Evasion: System Checks	Red Wolf checks the compromised system to identify a virtual environment
	Virtualization/Sandbox Evasion: Time Based Evasion	Red Wolf collects information on the time passed since the latest OS launch preceding the launch of the malware sample
Persistence	Scheduled Task/Job: Scheduled Task	Red Wolf creates a task in the scheduler to gain persistence in the compromised system
Discovery	System Information Discovery	Red Wolf collects information on the compromised system, including the username, the computer name, and the domain name
	File and Directory Discovery	Red Wolf collects information on the files and folders in Program Files, Desktop and AppData\Local
Command and Control	Application Layer Protocol: Web Protocols	Red Wolf uses `HTTP` and `HTTPS` to communicate with the C2 servers

Indicators of compromise

- `e7b881cd106aefa6100d0e5f361e46e557e8f2372bd36cefe863607d19471a04`
- `3bd054a5095806cd7e8392b749efa283735616ae8a0e707cdcc25654059bfe6b`
- `4188c953d784049dbd5be209e655d6d73f37435d9def71fd1edb4ed74a2f9e17`
- `app-ins-001.amscloudhost[.]com`
- `m-dn-001.amscloudhost[.]com`
- `m-dn-002.amscloudhost[.]com`

Detailed information about Red Wolf, its tactics, techniques, and procedures, as well as more indicators of compromise are available with BI.ZONE ThreatVision.
