Threat Thursday: NetWire RAT is Coming Down the Line

RESEARCH & INTELLIGENCE / 09.16.21 / The BlackBerry Research and Intelligence Team

NetWire is a publicly available, multi-platform Remote Access Trojan (RAT) that is designed to target victims on Windows®, MacOS®, and Linux®. This threat has been distributed in phishing campaigns via weaponized Microsoft® documents, PDFs containing download links, and archive files containing payloads. It has also been seen for sale on the dark net, typically ranging in price from $40 to $140 USD.

The goal of NetWire is to perform surveillance or take control of the infected system. Once the RAT has compromised a machine, the attacker can execute a variety of remote actions from its command and control (C2) server.

The malware's surveillance abilities include logging keystrokes, capturing screenshots, and stealing passwords, as well as accessing web cameras and microphones.

Operating System

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

Cookie Settings Decline Accept

Impact	**Medium**
Risk	**Medium**

Technical Analysis

NetWire was first discovered in the wild in 2012, and it has been used since then by financially motivated cyber-criminals, as well as advanced persistent threat (APT) groups.

Typically, the infection vector used to distribute this malware is via phishing campaigns where victims are lured into clicking on malicious Microsoft® Office files that contain embedded macros, which then launch a payload. The malware has also been seen spreading via malicious URLs in PDF files, as well as through malicious attachments in emails.

The variant analyzed in this report was a binary created to target Windows machines. The file would arrive as a Win32 executable that is UPX-packed to help impede analysis.

The malware also uses an anti-analysis technique to avoid execution in a sandbox. The “GetCursorPos” function is called twice, as seen below, and the cursor positions are compared. The malware will not run until there is a difference in the mouse cursor positions.

```
003E005A    FFD0            call eax                        GetCursorPos
003E005C    83F8 00         cmp eax,0
003E005F    0F84 4F1E0000   je 3E1EB4
003E0065    0F6F0424        movq mm0,qword ptr ss:[esp]
003E0069    6A 01           push 1
003E006B    FF95 94000000   call dword ptr ss:[ebp+94]      sleep
003E0071    54              push esp
003E0072    FF95 08010000   call dword ptr ss:[ebp+108]     GetCursorPos
```

Figure 1: Anti-sandbox technique

These are not the only tricks NetWire uses to hide its activity. When executed, the malicious binary creates a child process, and its code is then overwritten into this process. Because this is where the malicious activity spawns from, this makes analysis more difficult.

The parent process drops the child process into the “User/AppData/Roaming/Install” directory and exits itself. This is shown in the image below, with the filename “Host.exe.”

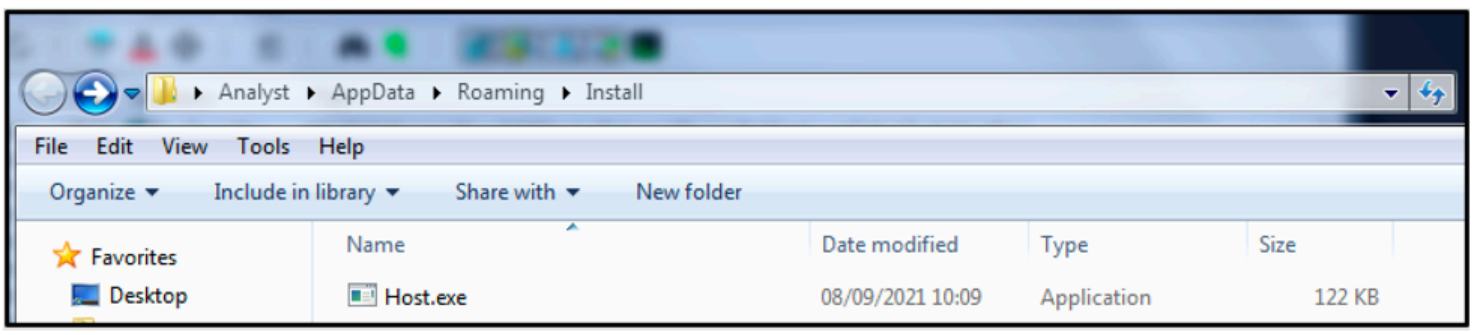

Figure 2: Copy of Host.exe in “User/AppData/Roaming/Install”

NetWire creates a registry key and adds it to the auto-run group to achieve persistence. This will ensure that the malicious file will run automatically when the victim’s machine is booted up.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

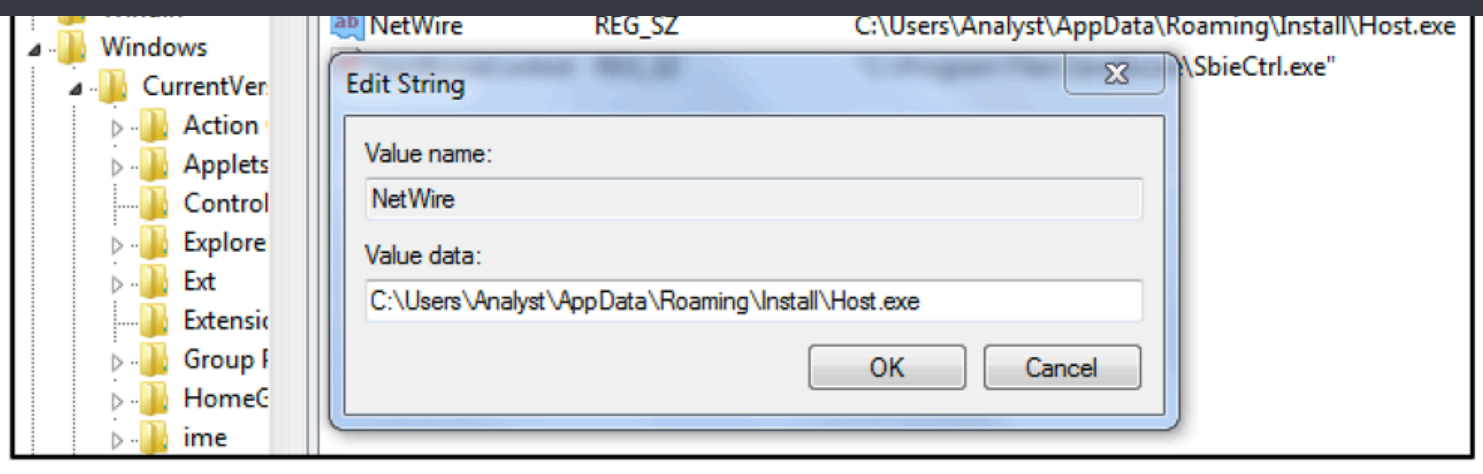

Figure 3: NetWire RegKey for maintaining persistence on victim's machine

By analyzing the strings in memory, we can see some of the functionality carried out by NetWire, and the information that it is attempting to gather.

It tries to gather user login data from web browsers such as Google Chrome™ and Brave® Browser.

0x41db1c	59	%s\BraveSoftware\Brave-Browser\User Data\Default\Login Data
0x41db58	48	%s\360Chrome\Chrome\User Data\Default\Login Data

Figure 4: NetWire browser credential-harvesting functionality

The malware also scans the directories of Microsoft® Outlook® profiles on the victim's machine to gather credentials. It also collects and logs both keystrokes and mouse movements.

The keystrokes are of particular interest to the attacker as a potential source of sensitive information that can be used for malicious activity or financial gain. This could include data such as login details for online banking sites, credit card information, corporate network access credentials, or crypto wallets. This harvested information can often fetch a hefty price on underground forums and the dark web.

NetWire creates a log file on the victim's machine in the "User/Analyst/AppData/Roaming/Logs" directory, where it stores all captured data. As shown below, the log file is named using the format DAY-MONTH-YEAR, matching the date the victim's machine was infected.

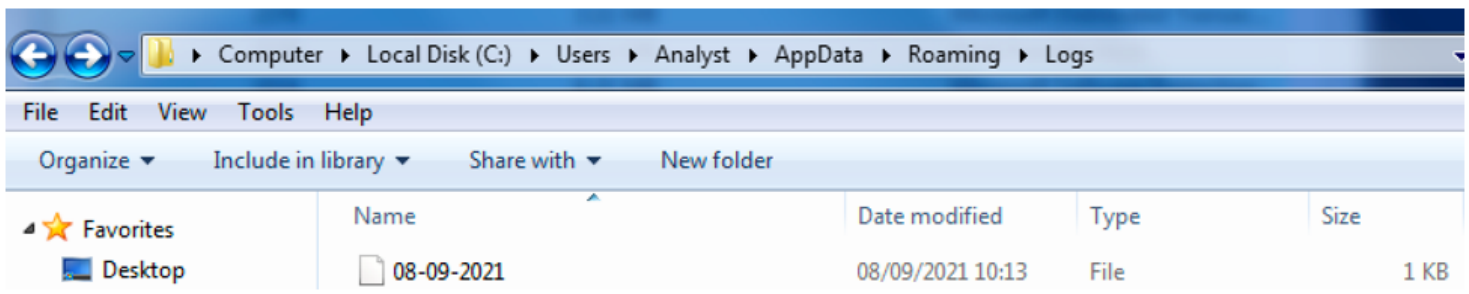

Figure 5: File created in the /Roaming/Logs directory, which contains all captured data

The data contained within the log file is encrypted using an RC4 cryptographic algorithm, the same algorithm the malware uses to encrypt strings and DLLs. NetWire also uses this obfuscation technique to hide registry keys, APIs, DLL names, and other strings.

Figure 6 shows the contents of the encrypted log file. The file grows larger the longer the malware remains on the machine, as it gathers more data.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

0x Hex File stats

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000060	02	E4	B4	BB	B4	BB	EA	F2	0D	20	13	0D	E1	14	1C	17	.....
00000070	0C	E4	E1	D4	E1	EA	D1	C9	D6	D1	C8	D6	D3	D1	D3	D0	.....
00000080	E1	D0	D1	CB	D2	D3	CB	CD	CF	E4	B4	BB	13	1C	1E	18	.....
00000090	12	0D	13	08	E1	1C	1D	18	0D	16	13	EA	03	20	22	1A	.....".
000000A0	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	..."....."...".
000000B0	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	03	20	22	...."...."....."
000000C0	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	...."....."...."
000000D0	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	03	20	....."....".....
000000E0	22	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	"...."....."...."
000000F0	22	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	03	"....."...."...."
00000100	20	22	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	."...."....."...
00000110	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	."....."...."...
00000120	03	20	22	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	12	.."...."....."..
00000130	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	.."....."...."..
00000140	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	..."...."....."
00000150	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	..."....."...".
00000160	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	EA	03	20	22	...."...."....."
00000170	1A	12	11	20	22	1C	E4	EA	03	20	22	1A	12	11	20	22	...."....."...."
00000180	1C	E4	EA	03	20	22	1A	12	11	20	22	1C	E4	13	1C	1E	....."....".....
00000190	13	1C	1E	13	1C	1E	18	12	0D	13	08	E1	1C	18	EA	03	.....
000001A0	20	22	1A	12	11	20	22	1C	E4	1D	18	0D	16	13	EA	FC	."....".....
000001B0	17	0D	1C	13	E4	B4	BB	B4	BB	EA	F1	13	16	1E	13	20	.....
000001C0	14	E1	F4	20	17	20	1E	1C	13	E4	E1	D4	E1	EA	D1	C9	.....
000001D0	D6	D1	C8	D6	D3	D1	D3	D0	E1	D0	D1	CB	D2	CC	CB	CC	.....
000001E0	D1	E4	B4	BB	13	1C	1E	B4	BB	B4	BB	EA	F2	0D	20	13	.....
000001F0	0D	E1	14	1C	17	0C	E4	E1	D4	E1	EA	D1	C9	D6	D1	C8	.....

Figure 6: Encrypted log file containing harvested data

The malware also creates a mutex called “OqvAvPni” on the target machine. This is used by the malware author to avoid reinfection of the same host.

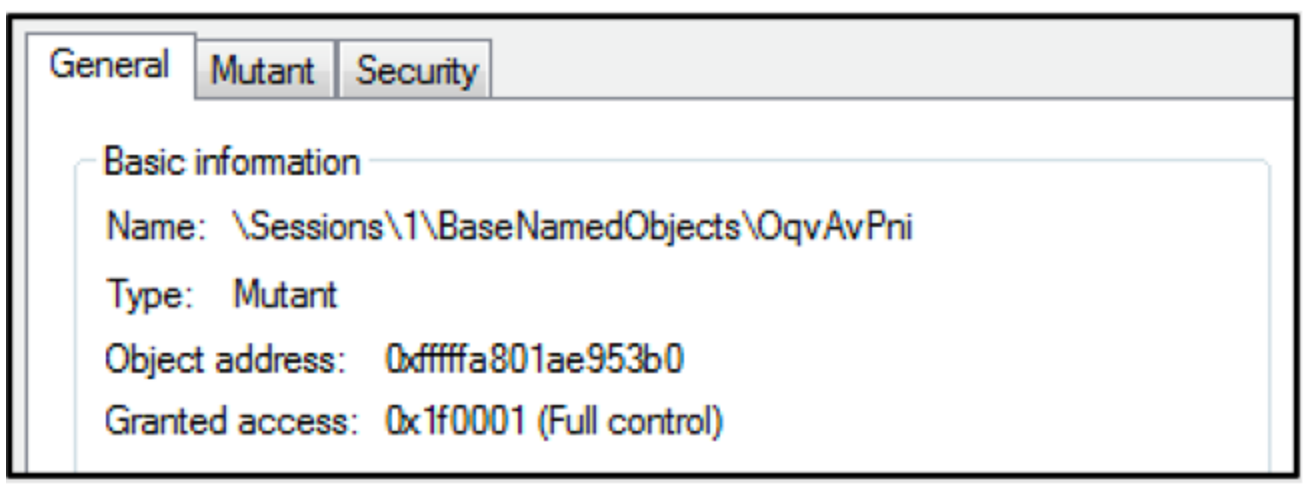

Figure 7: Mutex “OqvAvPni” created by NetWire

NetWire will attempt to create a TCP connection with a remote C2 server. In the sample used in this analysis, there were continuous attempts to create a connection over port 3382 with the IP Address 192[.]169[.].69[.]25.

From the strings in memory, we can see the DNS of the C2 server that this variant is attempting to reach is “love82[.]duckdns[.]org”.

0x4b51ac	36	love82.duckdns.org

Figure 8: C2 URL “love82[.]duckdns[.]org” visible in strings in memory

If this connection is successful, the attacker can transfer captured data or perform further malicious actions, such as downloading and executing additional malicious payloads.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

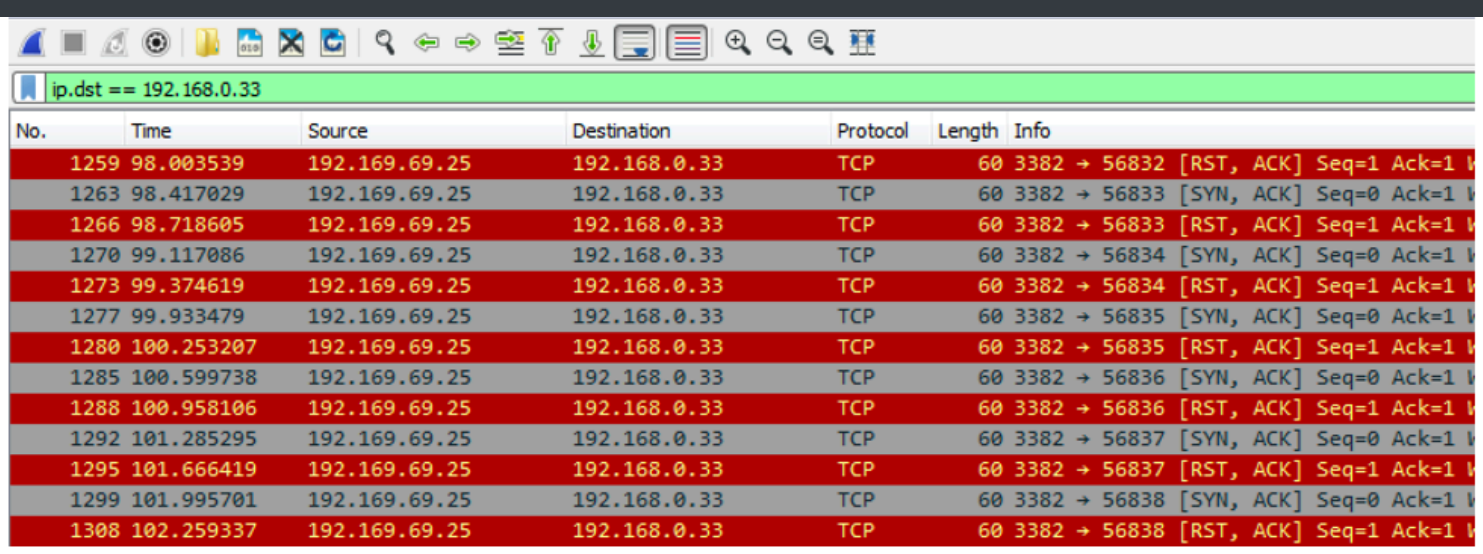

Figure 9: Wireshark results showing continuous TCP connection attempts with C2

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"
rule NetWire_RAT {
  meta:
    description = "Detects NetWire Remote Access Trojan"
    author = "BlackBerry Threat Research Team"
    date = "2021-09-06"
    SHA256 =
"021323e02e618769aab03cd9d5dea602ff684c2ff64ef592d69b119e78502fd9"

  strings:
    $s1 = "test.exe"
    $s2 = "key_dtor_list"
    $s3 = "new_key"
    $s4 = "./mingw-w64-crt/crt/natstart.c"
    $s5 = "./mingw-w64-crt/crt/tlssup.c"
    $s6 = "./mingw-w64-crt/crt/tlsmcrt.c"
    $s7 = "cygming-crtbegin.c"
    $s8 = "tagCOINITBASE"
    $s9 = "IID_IWinInetFileStream"
    $s10 = "winnt.h"
    $s11 = "fwrite"

  condition:
    ( uint16(0) == 0x5a4d and filesize < 1500KB and
      pe.imphash() == "084fafd5fea9d39b4ff35f2d82f0908b" and pe.number_of_sections
== 15 and ( all of them )
    )
}
```

Indicators of Compromise (IoCs)

SHA256

- 021323e02e618769aab03cd9d5dea602ff684c2ff64ef592d69b119e78502fd9

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

C2

- 192[.]169[.].69[.]25

Mutex

- OqvAvPni

Registry

- HKCU\SOFTWARE\NetWire

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you with around-the-clock support, if required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research and Intelligence Team

The BlackBerry Research and Intelligence team is a highly experienced threat research group specializing in a wide range of cybersecurity disciplines, conducting continuous threat hunting to provide comprehensive insights into emerging threats. We analyze and address various attack vectors, leveraging our deep expertise in the cyberthreat landscape to develop proactive strategies that safeguard against adversaries.

Whether it's identifying new vulnerabilities or staying ahead of sophisticated attack tactics, we are dedicated to securing your digital assets with cutting-edge research and innovative solutions.

Corporate

Company

Newsroom

Investors

Developers

Enterprise Platform & Apps

BlackBerry QNX Developer Network

Legal

Overview

Accessibility

Patents

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**

© 2024 BlackBerry Limited. All rights reserved.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. **Learn More**