THREATS

WarzoneRAT Evades Detection With Process Hollowing Technique

May 31, 2022

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-

The Uptycs Threat Research Team contributed to the profile of WarzoneRAT (S0670) in the MITRE ATT&CK framework, detailing the techniques and functionality of the malware.

Malware Operation

A depiction of the kill chain used by WarzoneRAT in one of the recently captured samples in our in-house osquery integrated threat intelligence sandbox is shown below (Figure 1).

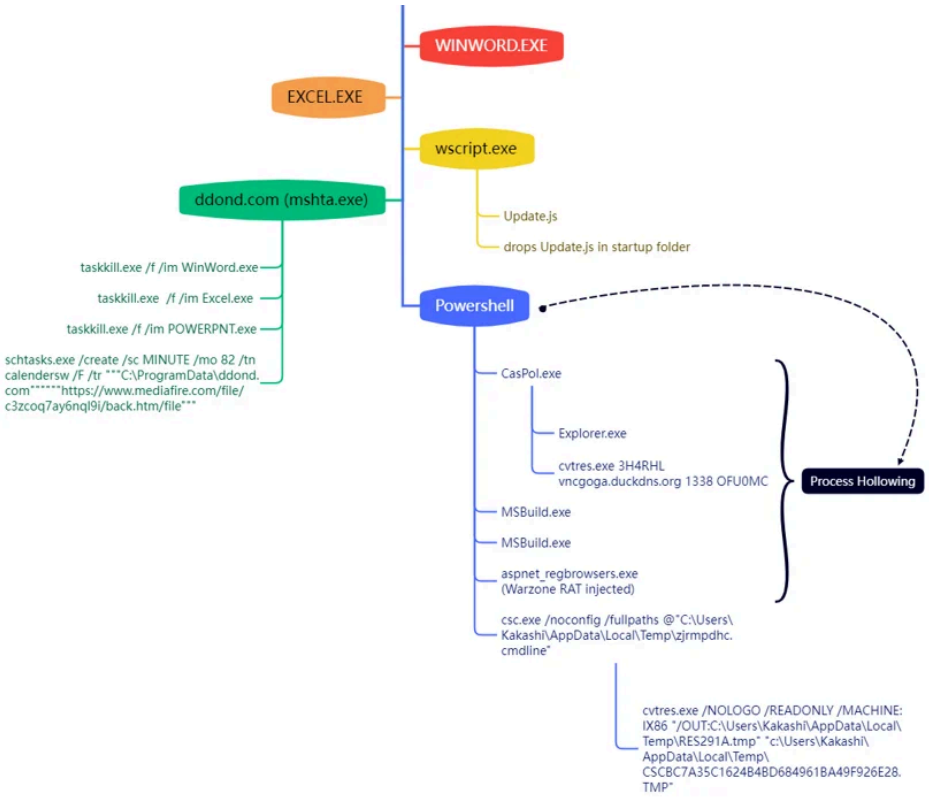

Figure 1: Attack Kill Chain of latest WarzoneRAT sample including process hollowing

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 technique as shown in Figure 1.
- It also launches csc.exe to compile .cs file on the fly into dll to decompress the compressed code for further execution.

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

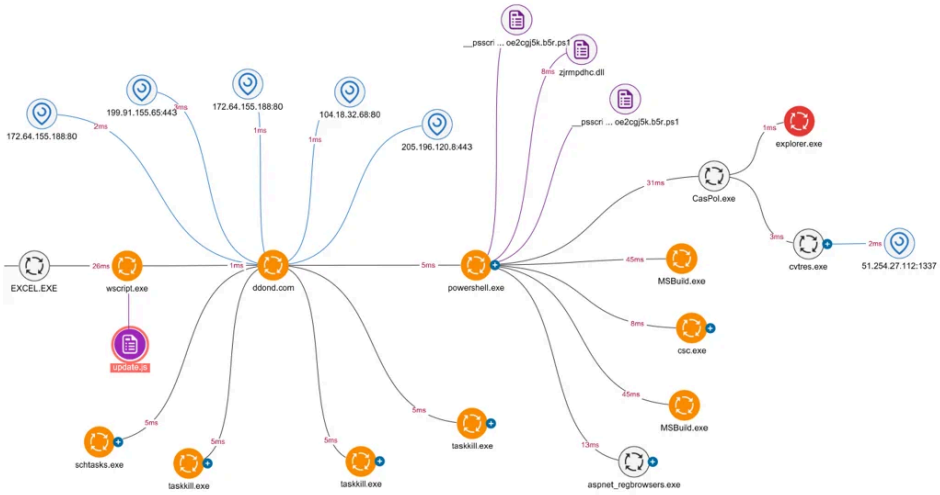

Figure 2: Uptycs Detection graph of WarzoneRAT

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:

Figure 3: Deobfuscated Powershell code using process injection in legit process

- The cmdlet executes the function “Execute” from the Class “projFUD.PA”.
- The “Execute” Function then uses process hollowing technique to inject malicious code into legit processes such as aspnet_compiler.exe, aspnet_regbrowsers.exe, CasPol.exe, RegAsm.exe and MSBuild.exe.

The API usage for the process hollowing is shown below (See Figure 4).

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

advanced detections and correlating Registry Events, Process File Events, Process Events and API Events successfully detects different types of tactics carried out by WarzoneRAT.

Additionally, Uptycs EDR contextual detection provides additional details about the detected malware. Users can navigate to the toolkit data section in the detection alert and click on the name to find out the behavior as shown as below (See Figure 6)

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,

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

Recommended Content

Investigating Threat Alerts With Osquery: Understanding Threat...

Stay in the loop

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

CNAPP Hybrid Cloud Security

Platform

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

By Platform

AWS

Microsoft Azure

Google Cloud

Integrations

Tools and Integrations

Why Uptycs

Why Choose Uptycs

About Us

Case Studies

Reviews

Compare Uptycs

Aqua

Lacework

Sysdig

CrowdStrike

Resources

Resources

Analyst Reports

Product Briefs

Blog

Video Hub

Threat Research Report Team

Whitepapers

E-books

Webinars and Events

Company

Careers

News

CSU

Support

Partners

Partner Program

Upward Partner Program