

# Threat Thursday: Warzone RAT Breeds a Litter of ScriptKiddies

---

[blogs.blackberry.com/en/2021/12/threat-thursday-warzone-rat-breeds-a-litter-of-scriptkiddies](https://blogs.blackberry.com/en/2021/12/threat-thursday-warzone-rat-breeds-a-litter-of-scriptkiddies)

The BlackBerry Research & Intelligence Team



## Executive Summary

---

- Warzone aims to be the Remote Access Trojan (RAT) of choice for aspiring miscreants on a budget. It is sold on a publicly available website as opposed to on the dark web, as a Malware-as-a-Service (MaaS) subscription-based platform. The initial subscription to the malware's basic RAT builder starts at only \$22.95 per month, a price-point which is more likely to attract novice threat actors (aka "script kiddies").
- Advanced features such as a rootkit, hidden process capability, premium dynamic DNS (DDNS), and customer support are available with the upgraded subscription. This premium version is called "Poison," and it's sold at a higher fee of \$879 for a three-month subscription.

- Threat actors can also choose to purchase builders for document-based exploit delivery, including a [recently disclosed 2021 XLL Excel exploit](#) that the malware author claims is fully undetected, for \$2100 per month.

## Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

## Risk & Impact

Impact	High
Risk	Medium

## Technical Analysis

Warzone is marketed as a “C++ Native RAT” built for Windows®, as seen in the image below of a post by @Solmyr of *Hack Forums*, which boasts of continuous updates, support, and reliability. The RAT first appeared in 2018 and has received several updates since then.

This threat is often called “*Ave Maria*” due to a string it uses, but analysis [by\\_yoroi](#) shows that the command-and-control (C2) was using Warzones’ DDNS at [anglekeys.warzonedns\[.\]com](#).

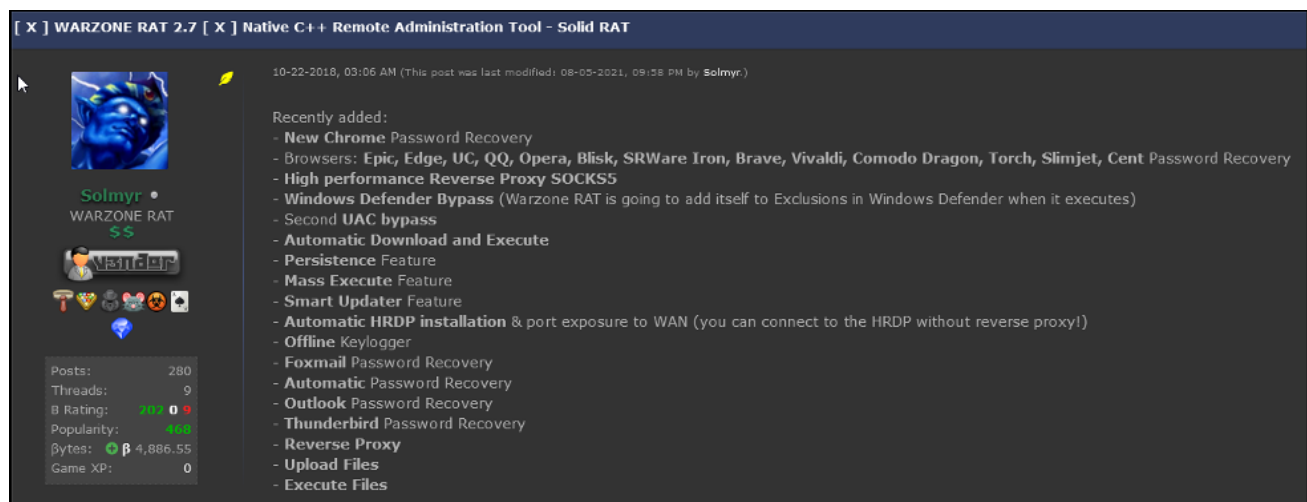


Figure 1 - Hack Forums posting

As is common with malware building kits like this, there are multiple versions that have been cracked and disseminated. These cracks often have Trojans or backdoors added, in which case it is necessary to handle analysis even more carefully.

The latest major builder release is Warzone 2.7, which brought a Hidden Remote Desktop Protocol (HRDP) update and support for Windows® 10 Home. HRDP functionality allows the attacker to access the system at the same time as the victim without alerting them. This version has been cracked (as shown in Figure 2) and is easily found on VirusTotal.

📁 Clients	11/23/2021 2:06 PM	File folder	
📁 Datas	11/23/2021 2:06 PM	File folder	
📁 Injector	11/23/2021 2:06 PM	File folder	
📄 cratclient.bin	8/28/2020 1:54 PM	BIN File	113 KB
📄 cratclientd.bin	8/28/2020 2:01 PM	BIN File	113 KB
📄 License.dll	3/25/2020 5:29 AM	Application extension	1,470 KB
📄 MaterialSkin.dll	6/5/2019 2:46 AM	Application extension	571 KB
📄 PETools.dll	5/2/2017 12:42 AM	Application extension	20 KB
🌀 Warzone Cracked	2/22/2021 5:01 AM	Application	529 KB
📄 Warzone Cracked.exe.config	2/22/2021 1:12 AM	CONFIG File	1 KB
PV WARZONE Password Viewer 1.0	6/28/2019 1:58 PM	Application	616 KB
📄 WARZONE RAT 2.70	8/27/2020 11:21 PM	Application	8,077 KB
📄 WARZONE RAT 2.70.exe.config	3/23/2019 12:23 PM	CONFIG File	2 KB


*Figure 2 - Cracked folder file listing*

This RAT is highly configurable. The malware operator can specify things like the IP address and port for the C2 server, as well as payload name, startup options, Alternative Data Stream (ADS) usage, and numerous other features as shown below.

Client Builder

Hostname :

Port :

Random String :  

Install     Use ADS install + startup

Install Name :

Startup

Startup Name :

Offline Logs

Persistence/Watchdog

Build as a DLL     Enable UAC Bypass

Bypass windows defender

Figure 3 - Configuration details pane

Changes that are made to the build options do not necessarily change the overall malicious code, per se. Instead, changes are reflected in a set of configuration information options that are stored in the build payload itself.

Due to this approach, the most recent release (2.7) builder produces all payloads with the following Import Hash: **51a1d638436da72d7fa5fb524e02d427**

The configuration information is stored in the BSS section RC4-encrypted, with the first dword being the length of the key, followed by the key, then the data in Unicode.

The payload of the configuration information (as of 2.7) has been decoded as follows. All flags are 01 if set, 00 if unset.

<b>Size</b>	<b>Description</b>
<b>dword</b>	Length (i) of C2 string
<b>i bytes</b>	C2 string
<b>dword</b>	C2 port (default 5200)
<b>dword</b>	Unused? – always all 0s
<b>byte</b>	Install option flag
<b>dword</b>	Length (j) of install name
<b>j bytes</b>	Install name
<b>byte</b>	Startup option flag
<b>dword</b>	Length (k) of startup name
<b>k bytes</b>	Startup name
<b>dword</b>	Local port for reverse proxy (default 5000)
<b>byte</b>	Offline Log flag
<b>byte</b>	Persistence/Watchdog flag
<b>byte</b>	UAC bypass flag
<b>byte</b>	Defender bypass flag

---

<b>byte</b>	ADS install + startup flag
-------------	----------------------------

---

<b>dword</b>	Length (l) of random string
--------------	-----------------------------

---

<b>l bytes</b>	Random string set by builder
----------------	------------------------------

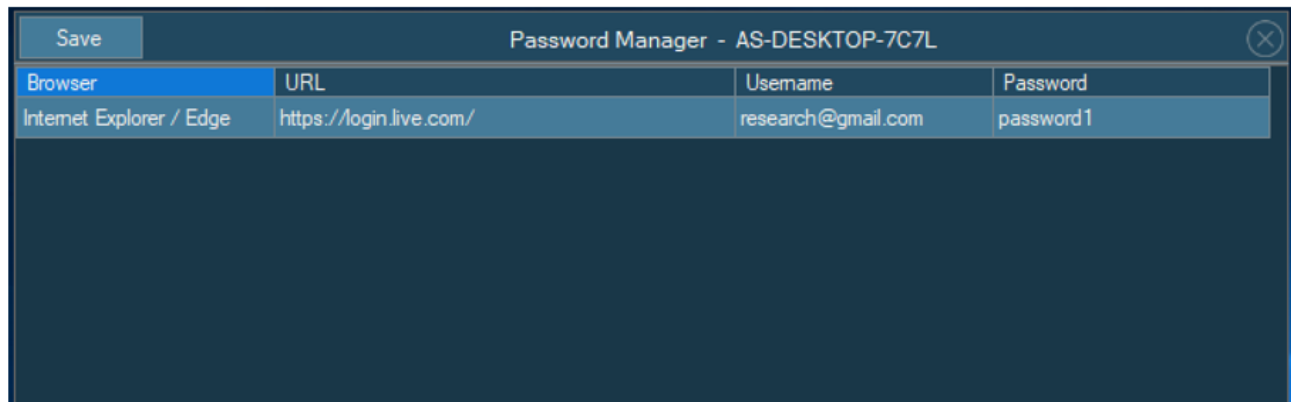


Figure 4 - Password capture management

Upon connection, the malware searches known file paths, as shown in Figure 4, for stored credentials that it can automatically harvest. This can allow an attacker to potentially score quick wins, such as escalating privileges or stealing financial information.

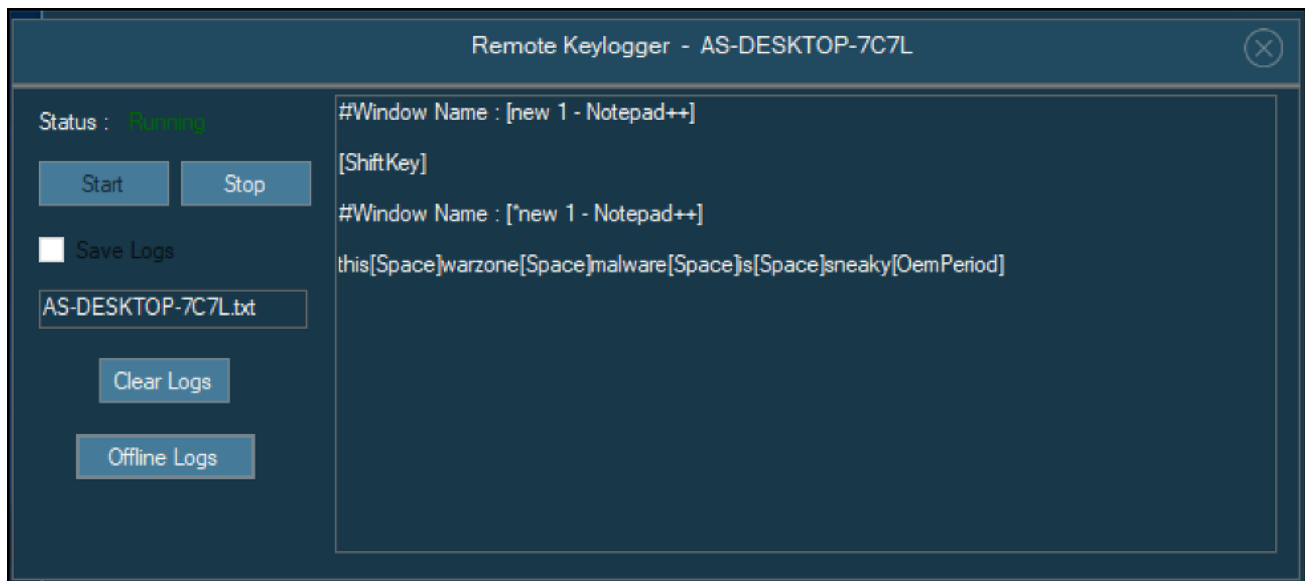


Figure 5 - Warzone keylogging

To extend the password stealing capacity, a silent keylogger (as shown in Figure 5) includes functionality to track which files are opened, and which control keys have been typed.

The keylogger can be set up to continue collecting logs when the victim is not connected. This is offered as an alternative to the automatic password stealer, allowing the malware operator to attempt to catch logins not stored in the system.

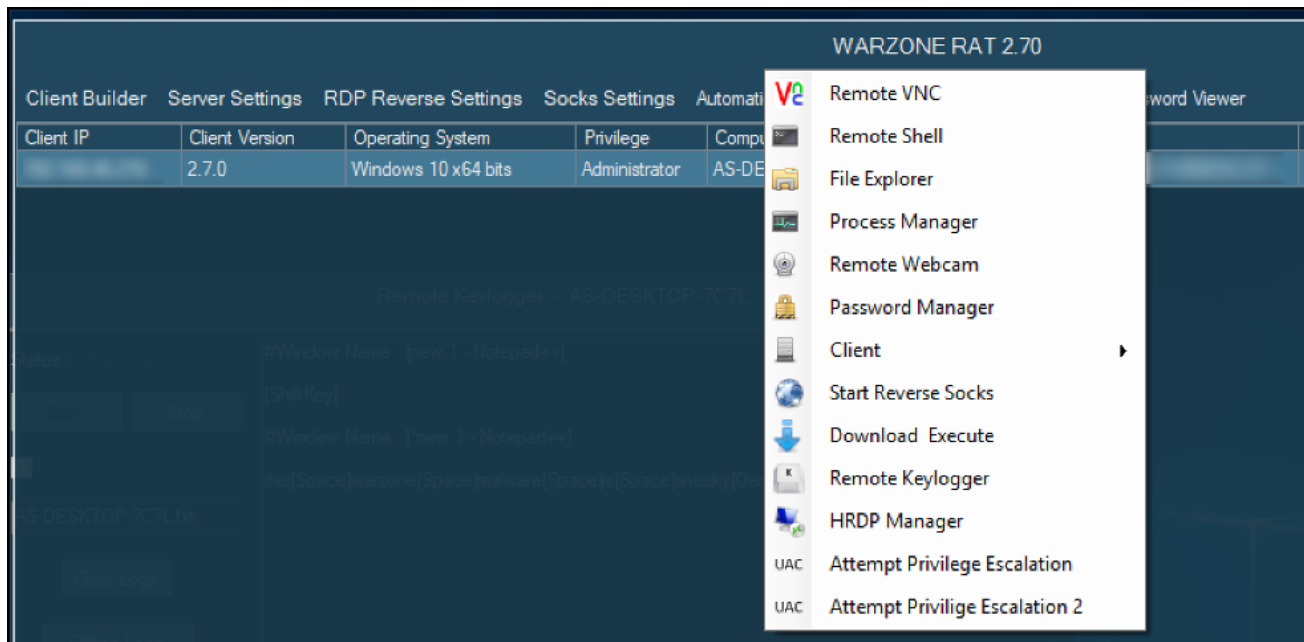


Figure 6 - Post exploit options menu

The post exploitation options menu contains many robust choices for stealing information/lateral movement. As shown in Figure 6 above, these options include the following:

- VNC connection
- Reverse Shell
- File explorer with option to download
- Process manager
- Remote webcam to access the victim's camera
- Password manager, configurable to dump stored credentials when the client connects
- Uninstall remote client
- Reverse SOCKS proxy
- Download and execute, to push further malware to the system
- Remote keylogger, configurable to continue storing keys when the client is offline
- Hidden RDP
- Privilege escalation options, in case the initial client was not configured to attempt these

If the malware was not already run with elevated privileges, it will attempt to escalate its privileges using an "sdclt" User Access Control (UAC) escalation. Sdclt is a file used in Windows systems to allow the user to perform backup and restore operations.

Sdclt is used to automatically elevate privileges by calling another copy of itself as a process with High Integrity level, bypassing the UAC prompt. Most program calls come from a context of Medium Integrity; with an sdclt process running in High Integrity, it is now less restricted on file and process access, as though it had been run by an administrator. This elevated process then calls control.exe – the Windows Control Panel – which then attempts to open the following registry key: HKCU\Software\Classes\Folder\shell\open\command.

Having done this, the malware sets the path to itself in this key, and it will now be run by the sdclt process.

When run as an already privileged user, the malware runs the command “powershell Add-MpPreference -ExclusionPath C:\” to create Windows Defender exclusions for the entire C drive. This exclusion ensures the malicious actor can move more malware on to the system without detection.

Persistence can be achieved by copying the payload to “%APPDATA%\Roaming” and writing a registry key in the path “HKCU\Software\Microsoft\Windows\CurrentVersion\Run.” This ensures that the RAT will be run again each time the user logs in, such as during a system restart. Warzone allows for customization of the install and startup names.

The malware also includes a configurable watchdog that will place a copy of itself in “%ProgramData%” that will run in the event of an unexpected termination.

On its own, the builder attempts no evasion, and generates payloads which are readily detected as malicious. To prevent such easy detection, many authors opt to use “crypters,” which are programs that obfuscate the true nature of the malware until runtime. This author has likewise written a crypter that is available for sale, which the author claims can bypass most antivirus (AV) products.

## **XLL Exploit**

---



## About XLL Excel Exploit

It's 2021 and it's time to introduce **new tools**.

Macros are less and less effective.

On this page you can learn about a tool which effectiveness will surprise you.

## Features

- **One click Excel Exploit**
  - FUD, check scan results: [Scantime & Runtime results](#)
- **Full coverage**

This exploit works on patched and unpatched office.  
Supported office versions: 2003, 2007, 2010, 2013, 2016, 2019, office365  
Supported Windows versions: XP, Vista, 7, 8, 8.1, 10, 11  
Architectures: 32 and 64 bits, builder can generate files for both architectures.
- **Custom Content**

You can insert content of your choice to the spreadsheet.
- **Regular updates**

We regularly check detection status and release updates when they're needed.
- **Professional Support**

If you need assistance - we are ready to help.  
Chat, TeamViewer, Anydesk  
**Our team has two new customer support specialists.**  
Their job is to provide you live support ASAP.
- **Bypass Windows Defender**
- **Bypass Smart Screen**
- **Bypass Gmail, Outlook, Yahoo**
- **Unlimited builds**

Figure 7 - Advertising for XXL Excel exploit delivery

The author of Warzone has also made an XLL exploit builder for sale, which could be used to embed a generated payload into an Excel file for delivery via phishing. While we were unable to obtain a copy of this builder, XLL files are typically add-in files that allow third-party code to add extra functionality to Excel. They are intended to be structured like DLL files and loaded in similar fashion.

The use of XLL files rather than traditional Excel XLS files for phishing is rare, so it's possible that malware authors may have taken notes from the Buer malware – which also uses XLL files – and complicated analysis by signing their files.

## **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 Mal_backdoor_Win32_WarzoneRAT_payload_2021
{
  meta:
    description = "Detects WarzoneRAT payload for latest builder (v2.7)"
    author = "Blackberry Threat Research Team "
    date = "2021-12"
    license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or
organization, as long as you use it under this license and ensure originator credit
in any derivative to The BlackBerry Research & Intelligence Team"

  strings:

    $string0 = "warzone160"
    $string1 = "PK11_Authenticate"
    $string2 = "dUser32.dll" wide
    $string3 = "\\logins.json" wide
    $string4 = "Account Name" wide
    $string5 = "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"
    $string6 = "NSSBase64_DecodeBuffer"
    $string7 = "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\" wide
    $string8 = "\\Slimjet\\User Data\\Default\\Login Data" wide
    $string9 = ":start" wide
    $string10 = "sqlite3_column_bytes"
    $string11 = "tG;HtsB"
    $string12 = "profiles.ini" wide
    $string13 = "\\Chromium\\User Data\\Local State" wide
    $string14 = "NtProtectVirtualMemory"
    $string15 = "ExplorerIdentifier" wide
    $string16 = "RtlGetVersion"

  condition:
    //Must be a PE File
    uint16(0) == 0x5a4d and

    //Must have specified imphash
    pe.imphash() == "51a1d638436da72d7fa5fb524e02d427" and

    //Must be greater then 95KB
    filesize > 95KB and

    //Must have the section name .bss
    pe.sections[pe.number_of_sections-1].name == ".bss" and

    //All Strings
    all of them
}

```

## Indicators of Compromise (IoCs)

---

**Warzone\_all\_hashes file:**

**String:** warzone160

**CommandLine:** powershell Add-MpPreference -ExclusionPath C:\

**Registry:** HKCU\Software\\_rptls

**ImpHash:** 51a1d638436da72d7fa5fb524e02d427

**SHAs:** (sample of 1.5k in Warzone\_all\_hashes file)

2944c31732655f1d470e483ab539c81e4fa0ec80b0f8753b4a856b0c894476e6

fcfd3248548efd7b521afddc86809165fd4b921f021130171335168247e7355b

b5d3060af008a045b96ff6362131d8b2f05d56f480cd5c01d960c21c4609b34a

a0584917b318ebeab9938cedabb1f2d184a33c5f33c2e6992968c9804360857f

9d56ad7e390d35d3fcf2bc03ac7b38e5efeee12e8bbc2917a375e6cf8c65d69f

066c455fd44d36695e2e0a97c41c25e8d2d21a90576f649159b16af4ffd860

5521c70600320df5bd5bbc6ef6ddc33f62e2078c7701452a60a58745adff1ffb

e85769eee5f2539084a2da5bf79027849249130be251d1f2e8b3de0021d194ab

b48c8a6fd76389cc51d279f896aa61d152212ce87b46a67b1171e3c40794eb4e

0968aac5baa3ca0333c06de5803c08300465441092fba720f9efe88f68cde4a0

5b6ac94ed2e8e2fda33d432f739588ad97db7a8865e51dc7ea2dc758eb1ed9cd

---

**MITRE ATT&CK Matrix TTPs**

The activities described in this report are mapped to the following MITRE ATT&CK® Matrix tactics, techniques, and procedures:

**Lateral Movement:**

T1021 – Remote Services - Remote Desktop Protocol and VNC available

**Collection:**

T1125 – Video Capture

**Collection, Credential access:**

T1056.001 – Input Capture: Keylogging

**Credential access:**

T1552.001 – Unsecured Credentials: Credentials in Files

**Execution:**

T1059.003 – Command and Scripting Interpreter: Windows Command Shell

**Persistence:**

T1137 – Office Application Startup

**Persistence, Privilege escalation:**

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

**Privilege escalation, Defense evasion:**

T1548.002 – Bypass User Account Control

**Exfiltration:**

T1041 – Exfiltration over C2 Channel

**Command-and-control:**

T1219 – Remote Access Software

**Discovery:**

T1083 – File and Directory Discovery

T1087 – Account Discovery

## **BlackBerry Assistance**

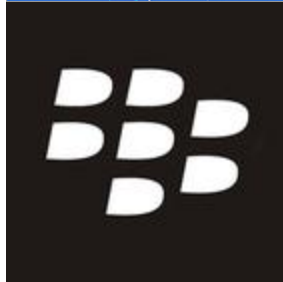
---

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 providing around-the-clock support, where 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 & Intelligence Team

---

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

---

[Back](#)