Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP: WHITE

2021-003: Ongoing campaign using Avaddon Ransomware

May 2021

The Australian Cyber Security Centre (ACSC) is aware an ongoing ransomware campaign utilising the Avaddon Ransomware malware. This campaign is actively targeting Australian organisations in a variety of sectors. This advisory provides details of Avaddon threat actors, dark web activity, targeted countries and sectors, the malware infection chain, and known Techniques, Tools, and Procedures (TTPs). If activity is identified relating to this advisory please report any findings to the ACSC (asd.assist@defence.gov.au).

Background

Avaddon is a ransomware variant first detected in February 2019, used in cybercriminal campaigns targeting multiple sectors and organisations around the world, including Australia. Avaddon is offered as a Ransomware-as-a-Service (RaaS), enabling affiliates to utilise it as desired, provided they return a percentage of profits to Avaddon developers as commission. The ACSC is aware of several instances where the Avaddon ransomware has directly impacted organisations within Australia.

Dark Web and Threat Activity

Avaddon has an active presence on underground dark web cybercrime forums, notably advertising the Avaddon RaaS variant to potential affiliates via a number of high tier cybercrime forums. Avaddon threat actors also utilise the data leak site (DLS) `avaddongun7rngel[.]onion` to identify victims who fail or refuse to pay ransom demands.

Avaddon threat actors demand ransom payment via Bitcoin (BTC), with an average demand of BTC 0.73 (approximately USD $40,000) with the lure of a decryption tool offered (‘Avaddon General Decryptor’) if payment is made.

Targeted Countries and Sectors

The ACSC is aware of active targeting of the following countries and sectors:

Targeted Countries	
Australia	Belgium
Brazil	Canada
China	Costa Rica
Czech Republic	France
Germany	Hawaii
India	Indonesia
Italy	Jordan
Peru	Poland
Portugal	Spain
United Arab Emirates	United Kingdom
United States	

Targeted Sectors	
Academia	Airlines
Construction	Energy
Equipment	Financial
Freight and Transport	Government
Health	Hospitality
Information Technology	Law Enforcement
Manufacturing	Marketing
Retail	Pharmaceutical
Virtual Entertainment	

Techniques, Tools, and Procedures

Identified Techniques, Tools and Procedures (TTPs) for Avaddon threat actors include:

- Using phishing and malicious email spam (malspam) campaigns to deliver malicious JavaScript files. These are often low in sophistication, containing a threat suggesting the attached file contains a compromising photo of the victim.
- Using ‘double extortion’ techniques as coercion and further pressure to pay a ransom including:
    - Threatening to publish the victim’s data (via the Avaddon Data Leak Site (DLS): `avaddongun7rngel[.]onion`
    - Threatening the use of DDoS attacks against the victim (identified since February 2021)
- Applying the GetUserDefaultLCID() function to identify the default geolocation and system language of the user’s device, subsequently, determining whether the user will be targeted for attack, or not. This technique has also been observed in ransomware campaigns using the MedusaLocker variant.
- TTPs for Avaddon are very similar to those identified in use within the Ako and MedusaLocker ransomware variants, including the use of an embedded public key to perform AES-256 encryption on all file data, as well as using a Windows Scheduled Task to establish persistence.

Malware Capabilities

The Avaddon ransomware has the following capabilities:

Allocates memory	Anti-VM capabilities	Anti-debug capabilities	Bypass Windows
Calculates FNV hashes	Capture FNV hashes	Capture Network Share information	Capture disk information
Capture hostname	Capture keyboard layout	Capture network configuration	Capture network interfaces
Capture operating system information	Capture payment card data	Capture system network information	Communicates using ICMP
Communicates using UDP	Communicates using raw sockets	Constructs mutex	Copy files
Create Windows registry key	Create Windows registry key value	Create files	Create thread
Creates processes	Decodes Base64	Delete Volume Shadow Copy files	Delete a service
Delete files	Encodes using Base64	Encodes using XOR	Executes using a scheduled task

Find files	Gets common file path	Gets environmental variable value	Gets file attribute
HTTP request capabilities	HTTP response capabilities	List file sizes	List files
Lists drives	Lists processes	Locks mutex	Move files
Open Windows registry key	Overwrite or wipe file data by emptying the Recycling bin quietly	Persistence via Windows registry Run key	Query service information
Read files	Reads memory	Receive data	Resolved Windows program files directory
Send data	Sets Wallpaper	Sets environmental variable	Sets file attribute
Start a service	Stop a service	Terminates processes	Uses AES
Uses AES256	Uses RC4	Uses RSA	Writes memory

MITRE ATT&CK

Technique ID	Name	Technique ID	Name
T1027	Obfuscated Files or Information	T147.001	Virtualisation/Sandbox Evasion / System Checks
T1202	Indirect Command Execution	T1078	Valid Accounts
T1562.001	Impair Defences: Disable or Modify Tools	T1070.004	Indicator Removal on Host/ File Deletion
T1486	Data Encrypted for Impact	T12082	System Information Discovery
T1120	Peripheral Device Discovery	T1490	Inhibit System Recovery
T1566	Phishing	T1498.001	Network Denial of Service / Direct Network Flood

Mitigations

The ACSC has published several products which can assist organisations in reducing the risk and impact of ransomware. These products can be found on the ACSC website, https://www.cyber.gov.au/ransomware.

The ACSC also recommends the following be implemented:

- Patch operating systems and applications, and keep antivirus signatures up to date.
- Scan emails and attachments to detect and block malware, and implement training and processes to identify phishing and externally-sourced emails.
- Maintain offline, encrypted backups of data and regularly test your backups. Regularly conduct backup procedures and keep backups offline or in separated networks.

Indicators of Compromise

SNORT Alert

```
Snort IDS: 2007837 ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (WinInet)
```

YARA Rules

```
TLP:WHITE] win_avaddon_w0 (20200902 | Detects Avaddon ransomware)
rule win_avaddon_w0 {
meta:
description = "Detects Avaddon ransomware"
author = "@VK_Intel, modified by @r0ny_123"
reference = "https://twitter.com/VK_Intel/status/1300944441390370819"
tlp = "white"
date = "2020-09-01"
malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.avaddon"
malpedia_rule_date = "20200902"
malpedia_hash = ""
malpedia_version = "20200902"
malpedia_license = "CC BY-SA 4.0"
malpedia_sharing = "TLP:WHITE"
strings:
$str0 = "rcid"
$str1 = "hdd"
$str2 = "lang"
$cfg_parser = { 55 8b ec 6a ff 68 74 d8 46 00 64 ?? ?? ?? ?? ?? 50 81 ec 3c 02 00 00 a1 ?? ?? ?? ?? 33 c5 89 ?? ?? 56 57 50 8d ?? ??
64 ?? ?? ?? ?? ?? 8b f1 89 ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ??
c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ??
8d ?? ?? ?? ?? ?? 8b ?? 51 8b ce ff ?? ?? 83 ?? ?? ?? ?? ?? ?? 0f ?? ?? ?? ?? ?? ?? 8d ?? ?? ?? ?? ?? 8d ?? ?? e8 ?? ?? ?? ?? c6 ?? ??
?? 8b ?? ?? 85 c0 0f ?? ?? ?? ?? ?? b9 10 00 00 00 c7 ?? ?? ?? ?? ?? ?? 3b c1 c7 ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 0f 42 c8 83 ?? ?? ??
8d ?? ?? 0f ?? ?? ?? 51 50 8d ?? ?? e8 ?? ?? ?? ?? c6 ?? ?? ?? 8b ?? ?? c7 ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 83 f8
10 0f ?? ?? ?? ?? ?? 83 c0 f0 b9 20 00 00 00 3b c1 0f 42 c8 83 ?? ?? ?? 8d ?? ?? 0f ?? ?? ?? 51 83 c0 10 8d ?? ?? 50 e8 ?? ?? ?? ??
c6 ?? ?? ?? 83 ?? ?? ?? 0f ?? ?? ?? ?? ?? 83 ?? ?? ?? 0f ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ??
c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c6 ?? ?? ?? 8d ?? ?? ?? ?? ?? 8b ?? 51 8b
ce ff ?? ?? 8b ?? ?? ?? ?? ?? 8d ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? 0f ?? ?? ?? ?? ?? ?? 0f ?? ?? ?? ?? ?? ?? f3 ?? ?? ?? ?? ?? ?? ?? 66
?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ??
?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ??}
$crypt_imp_seq_0 = { 83 ?? ?? ?? 8b c7 c7 ?? ?? ?? ?? ?? ?? 72 ?? 8b ?? 6a 00 6a 00 8d ?? ?? 51 6a 00 6a 01 6a 00 50 ff ?? ?? ?? ??
?? 85 c0 [3-6] 8b ?? ?? ff ?? ?? ?? ?? ?? 56 6a 00 50 ff ?? ?? ?? ?? ?? 8b f0 85 f6 [2-6] 83 ?? ?? ?? 72 ?? 8b ?? 6a 00 6a 00 8d ??
?? 50 56 6a 01 6a 00 57 ff ?? ?? ?? ?? ?? 85 c0 74 ?? [0-3] 8d ?? ?? 50 6a 00 6a 00 ff ?? ?? 56 ff ?? ?? ff ?? ?? ?? ?? ?? }
condition:
uint16(0) == 0x5a4d and 1 of ($str*) and ($cfg_parser or $crypt_imp_seq_0)
```

SHA256 Hashes

Hash Type	Hash
SHA256	0a052eff71641ff91897af5bdecb4a98ed3cb32bcb6ff86c4396b1e3ceee0184
SHA256	0ff4058f709d278ed662719b9627618c48e7a656c59f6bfecda9081c7cbd742b
SHA256	146e554f0d56db9a88224cd6921744fdfe1f8ee4a9e3ac79711f9ab15f9d3c7f
SHA256	165c5c883fd4fd36758bcba6baf2faffb77d2f4872ffd5ee918a16f91de5a8a8
SHA256	28adb5fa487a7d726b8bad629736641aadbdacca5e4f417acc791d0e853924a7
SHA256	2946ef53c8fec94dcdf9d3a1afc077ee9a3869eacb0879cb082ee0ce3de6a2e7
SHA256	29b5a12cda22a30533e22620ae89c4a36c9235714f4bad2e3944c38acb3c5eee
SHA256	331177ca9c2bf0c6ac4acd5d2d40c77991bb5edb6e546913528b1665d8b501f3
SHA256	46a8c1e768f632d69d06bfbd93932d102965c9e3f7c37d4a92e30aaeca905675
SHA256	5252cc9dd3a35f392cc50b298de47838298128f4a1924f9eb0756039ce1e4fa2
SHA256	61126de1b795b976f3ac878f48e88fa77a87d7308ba57c7642b9e1068403a496

Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
RED	Access to and use by your ACSC security contact officer(s) only. You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC security contact officer(s).
AMBER	Restricted internal access and use only. Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	Restricted to closed groups and subject to confidentiality. You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	Not restricted. WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
NOT CLASSIFIED	Any information received from ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC.