2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

WHO PLAYS ON AZORULT? AN UNKNOWN ATTACKER COLLECTS VARIOUS DATA AND SPREADS ADDITIONAL PAYLOADS WITH AZORULT FOR AROUND FIVE YEARS

Masaki Kasuya

BlackBerry, Japan

mkasuya@blackberry.com

ABSTRACT

In the cybersecurity space, security practitioners and researchers try to analyse malware based on deep-dive analysis and short-term trend research and we use the results of these to understand each malware behaviour and attack trend. In contrast, we rarely look at long-term trends, which usually provide us with interesting insights. For example, a single attacker uses a malware family's bot network to spread additional payload and/or steal sensitive information over a long period of time. Unfortunately, the C2 server does not send any response if we send invalid data, and C2 communication tends to be encrypted. Unless we are able to understand the whole procedure of C2 communication, we cannot track the C2 infrastructure for long-term analysis.

As a case study, this paper presents the results of long-term analysis of AZORult, an information stealer first analysed in 2016, whose C2 servers we started to track in January 2019. To this end, we implemented an AZORult emulator, which allowed us to get a valid data blob which contained commands from AZORult's C2 server. Overall, the stealer has been reducing its activity recently. However, we also revealed that an unknown attacker has been using AZORult's bot network to spread additional payloads and steal sensitive information for around five years. Based on our analysis, since it appeared the attacker has stolen information mainly related to cryptocurrency, password managers and multi-factor authentication. In addition to this, the attacker spread additional payloads via AZORult twice: From November 2019 to March 2020 and from June 2020 to March 2022. During the second additional payload campaign, we found that the attacker spread the same additional payloads on AZORult and Raccoon bot networks. This shows an attacker can use the same bot network for a long time and different bot networks to spread the same malware samples.

1. INTRODUCTION

Security researchers and practitioners often provide deep-dive analyses of particular malware families, generally focusing on the indicators of compromise (IoC) and behaviours of an individual sample or a few selected samples. These results contain valuable information from a defensive perspective, but they are just one perspective and can often be short lived as malware families periodically evolve. While deep-dive analyses offer immediate insights, long-term trend analysis can unveil more comprehensive understandings, shedding light on the strategies and operations of the malicious actors behind these botnets. Unfortunately, long-term trend analysis of malware is very challenging. Malware tends to update itself, and its C2 communication protocols also change with the updates. In addition, C2 communication is usually encrypted or encoded, and without identifying its decryption/decode algorithm, we cannot investigate the long-term trends of the malware efficiently.

This paper presents as a case study the results of long-term trend analysis of AZORult – an information stealer first discovered in 2016 [1] and thus considered an aged information stealer family. However, a few C2 servers are still active at the time of writing of this paper. In order to understand AZORult's long-term attack trend, we collected 2,364 C2 URLs, sent dummy check-in requests and received an encrypted binary blob which contained configuration data since 27 January 2019. We discovered that, although AZORult itself has reduced its activity recently, an attacker has used AZORult's bot network for around five years, with additional payloads being spread in two campaigns: from 4 November 2019 to 28 February 2020, and from 9 June 2020 to 21 March 2022. During the second campaign, the attacker also used the Raccoon stealer bot network to spread the same additional payloads found on AZORult bot network.

2. AZORULT C2 COMMUNICATION

In 2019, security researchers revealed the C2 communication protocol of AZORult [2]. To communicate with its C2 server, AZORult sends a check-in request based on the machine GUID, product name, username and computer name on the victim environment, as shown in Figure 1. The detailed algorithm of the ID generation is described in [2].

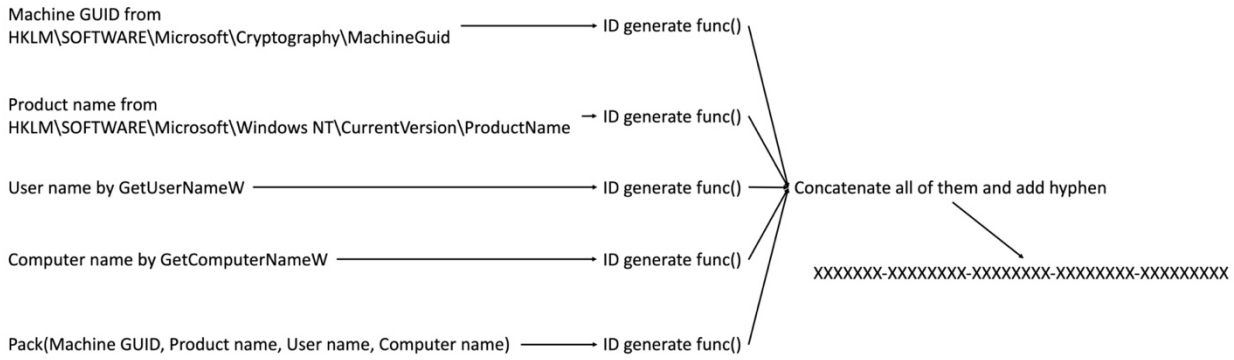

Figure 1: ID generation for check-in request (modified Figure 2 in [2]).

Once the C2 server accepts the initial check-in request, it returns an encrypted binary blob, the structure of which is shown in Figure 2. While this shows an example of AZORult v3.3 data format, its older versions are also similar data format. The

most interesting part is the data surrounded by the <c> tag. The data within the <c> tag is command data, which contains the target information the attackers want to steal and URLs to download and execute additional payloads.

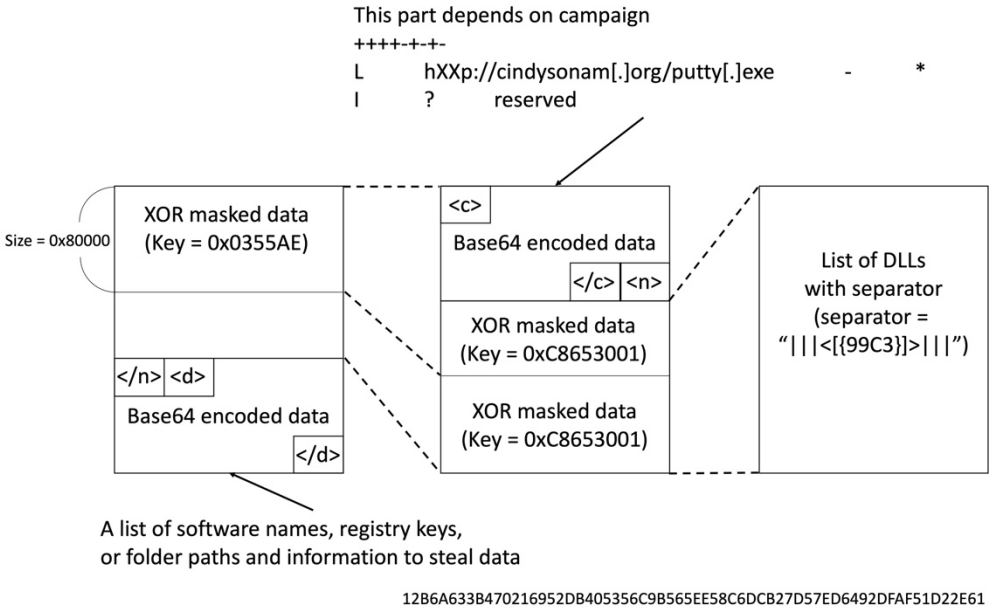

Figure 2: Configuration data format (v3.3) (Figure 3 in [2]).

An example of a command from AZORult's C2 server is shown in Figure 3. The first character of each line (i.e. 'F', 'L' and 'I') is the command type. 'F' specifies the target files the attackers want to steal. 'L' specifies the URLs for additional payload. 'I' is the victim computer's IP address and country name. A more detailed description of each command is available at [3].

```
From http://3e249703.ngrok.io/3/index.php

F 2 %USERPROFILE%\Documents\ *.txt,*.doc*,*.xls* 30+ +
F 1 %USERPROFILE%\Desktop\ *.txt,*.doc*,*.xls* 30+ +
L http://3e249703.ngrok.io/winrar.exe + test
I 9[redacted]3:US
```

Figure 3: Commands from AZORult C2 server.

3. IMPLEMENTATION

The implementation of the AZORult emulator is based on AZORult's C2 communication protocol as described in Section 2. It creates a dummy check-in request by randomly generating a disposable ID and sends it to the C2 server. Once the C2 server accepts the dummy request, it returns an encrypted binary blob. Depending on the AZORult version, the emulator decrypts and decodes the binary blob accurately. Currently, the implementation supports versions 3.2 and 3.3. This focus is sufficient because earlier versions are likely no longer active, and other researchers have similarly concentrated on tracking versions 3.2 and 3.3 since 2019 [4].

The emulator is implemented in Python 3 and deployed on Ubuntu 18.04.6 LTS with 4.15.0-213-generic kernel, 8 GB RAM and Intel(R) Core (TM) i5-7260U CPU @ 2.20GHz (2 cores). All network traffic goes through a VPN network [6].

4. EVALUATION

In order to investigate the long-term attack trend, the AZORult emulator has sent dummy requests to 2,364 C2 servers twice a day and collected configuration data from AZORult C2 servers since 27 January 2019. During this project, AZORult spread 1,237 unique samples belonging to 70 families via its bot network.

The following sections show first the macro trend of AZORult's activity, and secondly an AZORult user's activity over a long period.

4.1. Macro trend

This section describes AZORult's macro attack trend and malware families spread via AZORult users. To track the macro trend, an intuitive indicator is the number of active C2 servers, as shown in Figure 4. The number of C2 servers was more

than 50 and attackers used AZORult actively until February 2020. After that, the number of active C2 servers decreased gradually. This means AZORult is no longer a major malware family. This result is not a surprise because today's attackers have many options to choose from, including sophisticated information stealer families like Raccoon, Vidar, Lumma, Redline, Risepro and so on. When compared to these contemporary information stealer families, AZORult may be considered less potent.

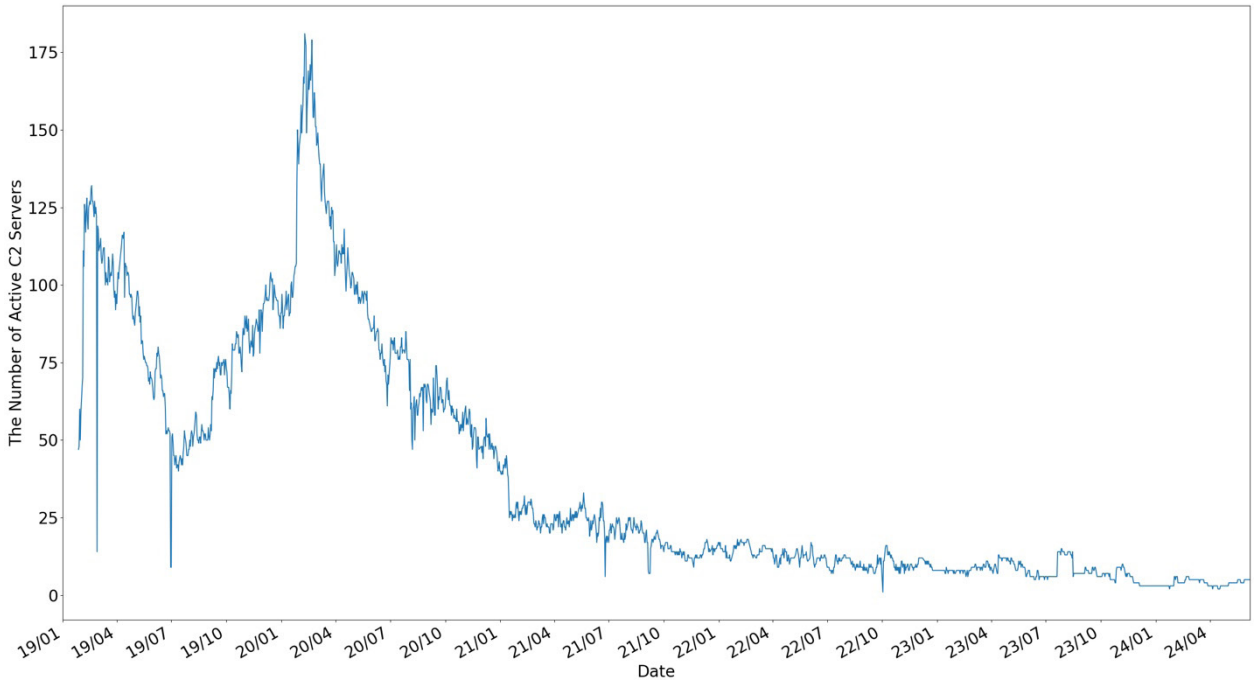

Figure 4: The number of active AZORult C2 servers.

Table 1 shows additional payloads spread via the AZORult bot network. As you can see, AZORult spread a variety of malware families including information stealers, remote access trojans, ransomware, and so on. During this project, the AZORult emulator collected 1,237 unique additional payloads. This result shows that the information stealer is also used as a loader to distribute other malware families. Indeed, it is known that many information stealers are also used as loaders to spread additional payloads – for example, Amadey, Redline, Raccoon, Vidar, RisePro and so on.

Blackout	Windows Defender Disabler	RMSRAT	OrcusRAT
Remcos	AsyncRAT	Clipper	QuilMiner
SmokeLoader	Predator Pain	Keylogger	Adamantium-Thief
GandCrab	KPOT	TinyNuke	ProstoClipper
ArechClient2	BlackRAT	XMRig	BrowserBot
ClipBanker	StealthWorker	N0f1l3 Stealer	ProtonBot
Blacknet	downloader	Neutrino Bot	BitRAT
AZORult	Qulab Clipper	CobaltStrike	QuilClipper
Petya	Qulab Stealer	TVRAT	Badut Clowns
Vidar	RevengeRAT	Phobos	Mighty Clipper
ParasiteHTTPRAT	Ursnif	Buran	Arcane
Netwire	AgentTesla	ServHelper	Sorano
Dropper	Redline	BetaBot	Echelon
hVNC RAT	DanaBot	Amadey	DarkComet
Coin Miner	QuasarRAT	Raccoon	Evrial
njRAT	PureMiner	OrionLogger	NanocoreRAT
Gootkit	WebMonitorRAT	AveMaria	SystemBC
Zyklon	Predator Stealer	DCRAT	

Table 1: Malware families spread via AZORult.

4.2 An AZORult user for 52 months

This section describes how an attacker used the AZORult bot network for around 52 months while AZORult itself was reducing its presence, as shown in Figure 3. Based on configuration data analysis, the attacker stole sensitive information with similar commands. In addition to this, the attacker spread additional payloads with similar families twice. Interestingly, the attacker also spread the same additional payloads via a different information stealer family.

4.2.1 Similarity among configuration data

In order to find the attacker who used the AZORult bot network over a long period, we investigated all configuration data collected by the AZORult emulator and realized the attacker had used a similar format for the 'F' command. Figure 5 shows two configurations from different AZORult C2 servers: the emulator received the top one on 4 November 2019 and the bottom one on 17 March 2024 (note that the configurations exclude some lines due to visibility). For example, see the similarity of the *DOC TXT* line in Figure 5. The two *DOC TXT* commands are similar. In addition to this, many other lines such as *Authy* have similar patterns in the two configurations.

```
From xcvzxf_ru/index[.]php (Received this configuration on 2019/Nov/14)
F  DOC TXT  %USERPROFILE%\Documents\ *.txt,150+  -
   \Windows\|\Program Files\|\Program Files (x86)\|\AppData\Local\|\AppData\LocalLow\|\AppData\Roaming\|\ProgramData\|\TEMP\|
   \PUBLIC\|\System32\|\Keygen\|\Crack\|\Patch\|\Games\|\Game\|\Downloads\|\Music\|\Movies\|\Mp3\|\Adobe\|\xampp\|\SteamGames\|\steamapps\
F  Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 +  -


From parals[.]ac[.]ug/index[.]php (Received this configuration on 2024/Mar/27)
F  DOC TXT  %USERPROFILE%\Documents\ *.txt 150+  -
   \Windows\|\Program Files\|\Program Files (x86)\|\AppData\Local\|\AppData\LocalLow\|\AppData\Roaming\|\ProgramData\|\TEMP\|
   \PUBLIC\|\System32\|\Keygen\|\Crack\|\Patch\|\Games\|\Game\|\Downloads\|\Music\|\Movies\|\Mp3\|\Adobe\|\xampp\|\SteamGames\|\steamapps\
F  Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 +  -
```

Figure 5: Configuration similarity.

Based on the findings, configurations from 95 C2 servers used the same tag names: *DOC TXT*, *Authy*, *Text*, *Desktop TXT*, *PNG*, *Winauth*, *JPG*, *Recent* and *PDF* for 52 months. To check the similarity of the contents tied with those tag names, we used Jaro-Winkler distance [5] for target files (e.g. *.txt) among the 95 configurations. The Jaro-Winkler distance is used to calculate the similarity of two strings.

Figure 6 shows the Jaro-Winkler distance of target files. The comparison source is the configuration data of xcvzxf[.]ru. The result means the configuration data from 95 C2 URLs have strong similarity. Based on the result, the 95 C2 URLs are tied with the same attacker.

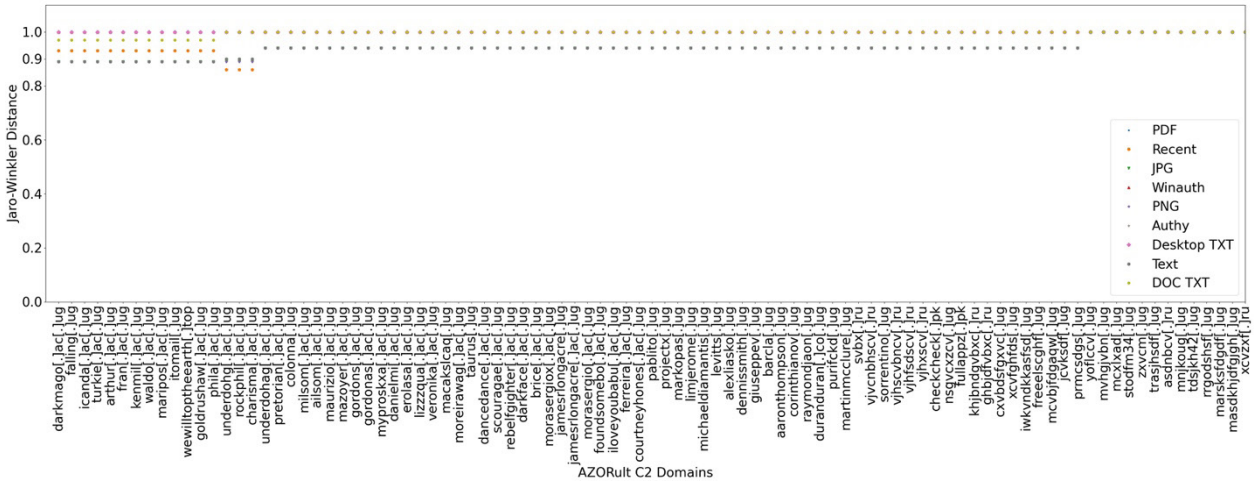

Figure 6: Jaro-Winkler distance of target files in command.

4.2.2. The attack campaign

During the course of almost 52 months, the attacker used 95 C2 URLs for their campaign. As shown in Figure 7, most of the C2 domains have a top level domain (TLD) of .ug. A portion of them have .ru domains and a few .pk and .top domains. Based on our analysis, the attacker operated four campaigns: the first was 14 November 2019 to 2 March 2020, the second was 5 March 2020 to 9 June 2020, the third was 9 June 2020 to 21 March 2022, and the fourth was 29 March 2022 to 27 March 2024.

The core motivation of the attacker was to steal sensitive information. Based on the configuration data analysis, the attacker collected data related to multi-factor authentication, cryptocurrency, and extracted passwords from password managers.

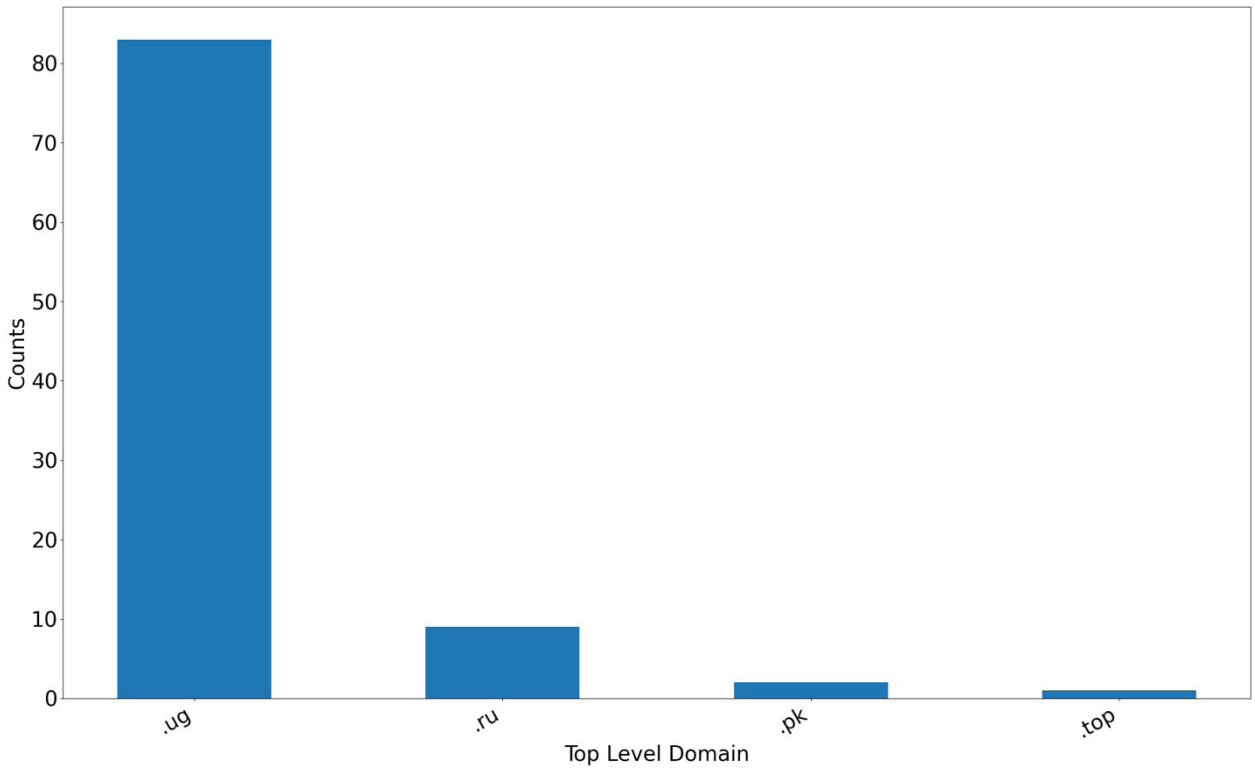

Figure 7: Top level domain of the C2 URLs for this campaign.

Table 2 shows the different payloads distributed in the first campaign. The attacker used Netwire and Windows Defender Disabler mainly, but also distributed Phobos ransomware for a short period. They also spread Kpot stealer and BlackRAT at the end of this campaign. The attacker predominately spread RAT-based malware and a tool to decrease *Windows* security settings. This trend was not only seen in the first campaign but also in the third campaign.

C2 domain	**Start date**	**End date**	**Additional payload**
xcvzxf[.]ru	2019/Nov/14	2019/Nov/15	Netwire
masdkhjdfgjgh[.]ug	2019/Nov/24	2019/Nov/25	Netwire
marsksfdgdf[.]ug	2019/Nov/28	2019/Dec/05	Netwire
rrgodshsf[.]ug	2019/Dec/02	2019/Dec/05	Netwire
tdsjkh42[.]ug	2019/Dec/11	2019/Dec/17	Netwire, Windows Defender Disabler
mnjkoug[.]ug	2019/Dec/16	2019/Dec/22	Netwire, Windows Defender Disabler
asdnbcv[.]ru	2020/Jan/03	2020/Jan/04	Phobos
trasjhsdf[.]ug	2020/Jan/27	2020/Jan/29	Phobos
zxvcm[.]ug	2020/Jan/28	2020/Jan/29	Netwire, Windows Defender Disabler
stodfm34[.]ug	2020/Jan/27	2020/Feb/03	Netwire, Windows Defender Disabler
mcxlxad[.]ug	2020/Jan/30	2020/Feb/03	Netwire, Windows Defender Disabler
mvhgjvbn[.]ug	2020/Feb/08	2020/Feb/11	Netwire, Windows Defender Disabler
yoflccv[.]ug	2020/Feb/08	2020/Feb/09	Netwire, Windows Defender Disabler
prmcsdgs[.]ug	2020/Feb/19	2020/Feb/25	Netwire, Kpot, BlackRAT
jcvksdf[.]ug	2020/Feb/28	2020/Mar/02	Netwire, Kpot, BlackRAT

Table 2: First campaign.

The second campaign started on 5 March 2020 and ended on 9 June 2020. During this campaign, the attacker stopped spreading additional payloads, as shown in Table 3.

C2 domain	Start date	End date	Additional payload
mcvbjfdgaqw[.]ug	2020/Mar/5	2020/Mar/5	N/A
freeelscghf[.]ug	2020/Mar/11	2020/Mar/12	N/A
iwkvndkkasfsd[.]ug	2020/Mar/17	2020/Mar/17	N/A
xcvfghfds[.]ug	2020/Mar/18	2020/Mar/27	N/A
cxvbdsfgxvc[.]ug	2020/Apr/6	2020/Apr/8	N/A
ghbjdfvbxc[.]ru	2020/Apr/11	2020/Apr/13	N/A
khjbndgvbxc[.]ru	2020/Apr/14	2020/Apr/15	N/A
fullappz[.]pk	2020/Apr/17	2020/Apr/21	N/A
nsgvcxzcv[.]ug	2020/Apr/25	2020/Apr/25	N/A
checkcheck[.]pk	2020/Apr/26	2020/Apr/26	N/A
vjhxscv[.]ru	2020/May/7	2020/May/9	N/A
vjhfsdscv[.]ru	2020/May/10	2020/May/13	N/A
vjhscvbncv[.]ru	2020/May/15	2020/May/19	N/A
sorrentino[.]ug	2020/May/14	2020/May/23	N/A
vjvcnbhscv[.]ru	2020/May/20	2020/May/25	N/A
svbx[.]ru	2020/May/24	2020/May/24	N/A
martinmcclure[.]ug	2020/May/25	2020/May/27	N/A
purifckd[.]ug	2020/May/28	2020/Jun/3	N/A
duranduran[.]co[.]ug	2020/Jun/4	2020/Jun/9	N/A

Table 3: Second Campaign.

In the third campaign, the attacker restarted spreading additional payloads, as shown in Table 4. They started by spreading Netwire, Windows Defender Disabler and Async RAT, and then switched Netwire to Remcos.

In June 2021, the attacker started spreading ClipBanker, after one month they stopped distributing Windows Defender Disabler and began spreading a coin miner in September 2021. The third campaign was longer than the first and the second campaigns, lasting around one year and nine months.

C2 domain	Start date	End date	Additional payload
raymondjaon[.]ug	2020/Jun/9	2020/Jun/15	Netwire, Async RAT
corinthianov[.]ug	2020/Jun/16	2020/Jun/21	Netwire, Windows Defender Disabler, Async RAT
aaronthompson[.]ug	2020/Jun/21	2020/Jun/25	Netwire, Windows Defender Disabler, Async RAT
barcla[.]ug	2020/Jun/25	2020/Jul/2	Netwire, Windows Defender Disabler, Async RAT
giuseppev[.]ug	2020/Jul/2	2020/Jul/8	Remcos, Windows Defender Disabler, Async RAT
dennissmith[.]ug	2020/Jul/9	2020/Jul/12	Remcos, Windows Defender Disabler, Async RAT
alexliasko[.]ug	2020/Jul/13	2020/Jul/13	Remcos, Windows Defender Disabler, Async RAT
levitts[.]ug	2020/Jul/15	2020/Jul/30	N/A
michaeldiamantis[.]ug	2020/Jul/31	2020/Aug/17	Remcos, Windows Defender Disabler, Async RAT
limjerome[.]ug	2020/Aug/17	2020/Aug/17	Remcos, Windows Defender Disabler, Async RAT
markopas[.]ug	2020/Aug/19	2020/Aug/26	Remcos, Windows Defender Disabler, Async RAT
projectx[.]ug	2020/Aug/27	2020/Aug/31	Remcos, Windows Defender Disabler, Async RAT
pablito[.]ug	2020/Sep/1	2020/Oct/26	Remcos, Windows Defender Disabler, Async RAT
courtneyhones[.]ac[.]ug	2020/Sep/7	2020/Sep/23	Remcos, Windows Defender Disabler, Async RAT
ferreira[.]ac[.]ug	2020/Sep/23	2020/Oct/4	Remcos, Windows Defender Disabler, Async RAT

Table 4: Third campaign.

C2 domain	Start date	End date	Additional payload
iloveyoubabu[.]ac[.]ug	2020/Oct/5	2020/Oct/8	Remcos, Windows Defender Disabler, Async RAT
foundsomebo[.]ac[.]ug	2020/Oct/10	2020/Oct/12	Remcos, Windows Defender Disabler, Async RAT, Raccoon
morasergio[.]ac[.]ug	2020/Oct/14	2020/Oct/14	Remcos, Windows Defender Disabler, Async RAT
jamesrlongacre[.]ac[.]ug	2020/Oct/15	2020/Oct/26	Remcos, Windows Defender Disabler, Async RAT
jamesrlongacre[.]ug	2020/Oct/28	2020/Nov/28	Remcos, Windows Defender Disabler, Async RAT
morasergiox[.]ac[.]ug	2020/Nov/20	2020/Dec/8	Remcos, Windows Defender Disabler, Async RAT
brice[.]ac[.]ug	2020/Dec/8	2020/Dec/23	Remcos, Windows Defender Disabler, Async RAT
darkface[.]ac[.]ug	2020/Dec/24	2020/Dec/31	Remcos, Windows Defender Disabler, Async RAT
rebelfgighter[.]ac[.]ug	2021/Jan/3	2021/Jan/4	Remcos, Windows Defender Disabler, Async RAT
scouragae[.]ac[.]ug	2021/Jan/5	2021/Jan/24	Remcos, Windows Defender Disabler, Async RAT
dancedance[.]ac[.]ug	2021/Jan/25	2021/Feb/9	Remcos, Windows Defender Disabler, Async RAT
taurus[.]ug	2021/Feb/10	2021/Jun/30	Remcos, Windows Defender Disabler, Async RAT
moreirawag[.]ac[.]ug	2021/Mar/31	2021/Apr/30	Remcos, Windows Defender Disabler, Async RAT
macakslcaq[.]ug	2021/May/2	2021/Jun/3	Remcos, Windows Defender Disabler, Async RAT
veronika[.]ac[.]ug	2021/Jun/4	2021/Jul/8	Remcos, Windows Defender Disabler, Async RAT, ClipBanker
lizzzqua[.]ac[.]ug	2021/Jul/2	2021/Jul/8	Remcos, Windows Defender Disabler, Async RAT, ClipBanker
erolasa[.]ac[.]ug	2021/Jul/9	2021/Jul/23	N/A
danielmi[.]ac[.]ug	2021/Jul/27	2021/Aug/16	N/A
myproskxa[.]ac[.]ug	2021/Aug/17	2021/Aug/17	Remcos, Async RAT
gordonas[.]ac[.]ug	2021/Aug/18	2021/Aug/18	Remcos, Async RAT, ClipBanker
gordons[.]ac[.]ug	2021/Aug/19	2021/Sep/2	N/A
mazoyer[.]ac[.]ug	2021/Sep/3	2021/Sep/17	Remcos, Async RAT, ClipBanker
maurizio[.]ac[.]ug	2021/Sep/18	2021/Oct/5	Remcos, Async RAT, ClipBanker, Miner
ailsom[.]ac[.]ug	2021/Oct/7	2021/Nov/4	Remcos, Async RAT, ClipBanker, Miner
milsom[.]ac[.]ug	2021/Oct/9	2021/Nov/2	Remcos, Async RAT, ClipBanker, Miner
colonna[.]ug	2021/Nov/3	2022/Feb/8	Remcos, Async RAT, ClipBanker, Miner
pretorian[.]ac[.]ug	2021/Dec/12	2022/Jan/7	Remcos, Async RAT, ClipBanker, Miner
underdohag[.]ac[.]ug	2022/Jan/11	2022/Mar/21	Remcos, Async RAT, ClipBanker, Miner

Table 4 contd: Third campaign.

During this campaign, the attacker used both AZORult and Raccoon bot networks to spread the same additional payloads at the same time. Table 5 shows additional payload information from both bot networks. The attacker used exactly the same file names, such as *rc.exe* and *ac.exe*, on both bot networks and the hash values were also exactly same. Based on those characteristics, the attacker tried to spread the same additional payloads on two bot networks.

In the fourth campaign, no additional payloads were spread, as shown in Table 6. Across all campaigns, the attacker utilized the AZORult bot network for 52 months. From a macro perspective, AZORult's activity is decreasing. However, malicious actors like this attacker can still effectively use even aged malware like AZORult.

Figure 8 shows the time to live (TTL) of the C2 URLs of all campaigns. During the first and second campaigns, almost all C2 URLs were active for less than a week. Therefore, the attacker changed C2 URLs frequently during the two campaigns. However, the active duration of C2 URLs during the third campaign was longer than the previous campaigns, with some URLs remaining active for more than a month. This shift to longer-lasting C2s is even more noticeable in the fourth campaign. While the attacker frequently changed their C2 URLs during the first, second, and third campaigns until the end of August 2020, in the fourth campaign they opted to maintain their C2 servers for extended periods.

Payload domain (via AZORult / Raccoon)	File name	Start date	End date
raymondjaon[.]ug / troygilletc[.]ug	nw.exe, ac.exe	2020/Jun/14	2020/Jun/15
corinthianov[.]ug / viniciuscorinthiano[.]ug	nw.exe, ac.exe, ds1.exe, ds2.exe	2020/Jun/16	2020/Jun/21
barcla[.]ug / gadem[.]ug	nw.exe, ac.exe, ds1.exe, ds2.exe	2020/Jun/25	2020/Jun/30
dennissmith[.]ug / smiothmadara[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Jul/9	2020/Jul/12
michaeldiamantis[.]ug / mantis[.]co[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Jul/31	2020/Aug/14
limjerome[.]ug / andreas[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/17	2020/Aug/18
markopas[.]ug / andreas[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/19	2020/Aug/25
projectx[.]ug / projectz[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/28	2020/Aug/28
pablito[.]ug / parajiti[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/1	2020/Sep/3
courtneyhones[.]ac[.]ug / courtneyjjones[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/7	2020/Sep/23
ferreira[.]ac[.]ug / ferreiranadii[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/23	2020/Oct/4
foundsomebo[.]ac[.]ug / letitburnsf[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Oct/10	2020/Oct/10
jamesrlongacre[.]ac[.]ug / 217[.]8[.]117[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Oct/15	2020/Oct/23
dancedance[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2021/Mar/31	2021/Mar/31
scouragae[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2021/Mar/31	2021/Mar/31
gordonas[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, cc.exe	2021/Aug/18	2021/Aug/18
ailsom[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, pm.exe, cc.exe	2021/Oct/23	2021/Oct/29
pretorian[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, pm.exe, cc.exe	2021/Dec/12	2021/Jan/7

Table 5: Payload distribution via AZORult and Raccoon.

C2 domain	Start date	End date	Additional payload
charisma[.]ac[.]ug	2022/Mar/29	2022/Apr/18	N/A
rockphil[.]ac[.]ug	2022/Apr/15	2022/Jun/8	N/A
underdohg[.]ac[.]ug	2022/Jun/2	2022/Jun/8	N/A
phila[.]ac[.]ug	2022/Jun/20	2022/Jul/10	N/A
goldrushaw[.]ac[.]ug	2022/Jul/12	2022/Aug/15	N/A
wewilltoptheearth[.]top	2022/Aug/15	2022/Sep/16	N/A
itomail[.]ug	2022/Sep/20	2022/Dec/18	N/A
maripos[.]ac[.]ug	2022/Oct/8	2022/Nov/26	N/A
waldo[.]ac[.]ug	2022/Nov/29	2023/Jan/13	N/A
kenmil[.]ac[.]ug	2023/Jan/16	2023/Mar/16	N/A
fran[.]ac[.]ug	2023/Jan/16	2023/May/27	N/A
arthur[.]ac[.]ug	2023/Feb/6	2023/Mar/20	N/A
turkie[.]ac[.]ug	2023/Apr/13	2023/Apr/17	N/A
icanda[.]ac[.]ug	2023/Apr/18	2023/May/10	N/A
falling[.]ug	2023/Jun/8	2023/Nov/10	N/A
darkmago[.]ac[.]ug	2023/Oct/27	2023/Nov/10	N/A
patatas[.]ac[.]ug	2023/Dec/23	2024/Jan/10	N/A
parals[.]ac[.]ug	2024/Feb/17	2024/Mar/27	N/A

Table 6: Fourth campaign.

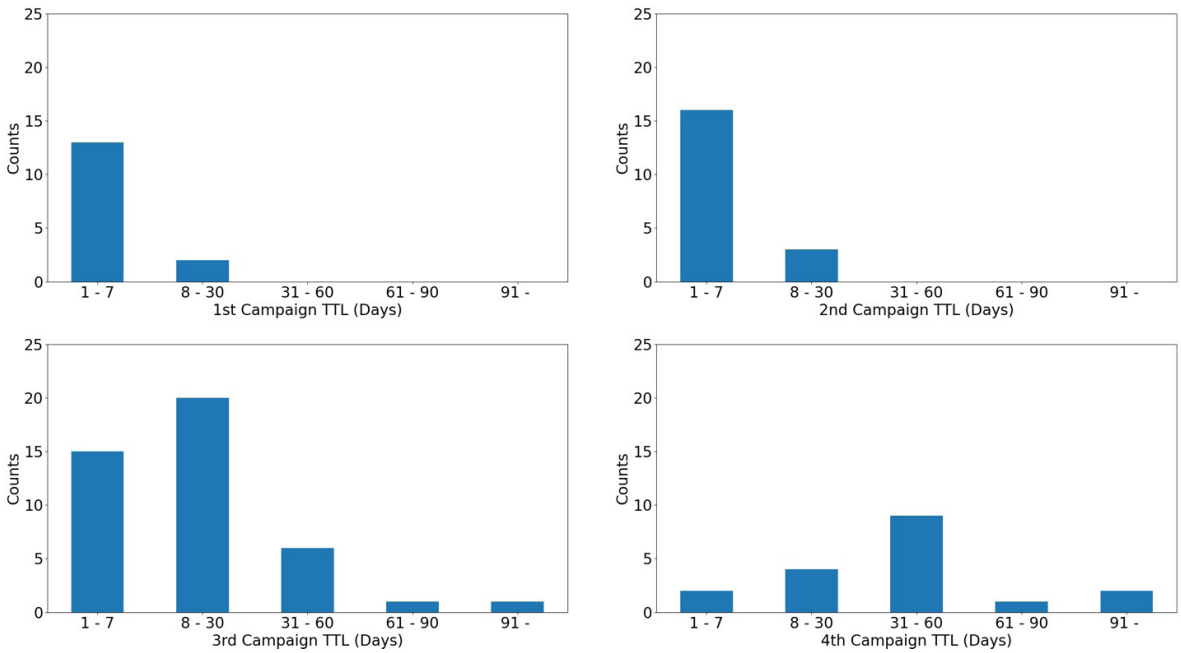

Figure 8: TTL of each C2 server per campaign.

Based on this result, security researchers and practitioners should take note that malware users like this attacker can use a bot network for a long time, even if the family itself is decreasing from the macro perspective.

5. DISCUSSION

This paper provides a long-term trend analysis of malware bot networks, using AZORult as a case study. From a macro perspective, AZORult activity has decreased significantly recently, but during this research, an attacker utilized the AZORult bot network for an extended period of time. If the cybersecurity community can allocate more resources to long-term trend analysis, it can provide valuable insights into the attackers that operate these malware bot networks. This understanding of attackers' intent and tactics enhances the capabilities of cyber threat intelligence.

In this work, the malware emulator collected configuration data from AZORult C2 servers. To minimize the risk of detection by the attackers, the emulator adjusts dummy information to mimic different victim environments. However, this emulator-based approach has limitations. First, if the malware botnet checks the IP address carefully, this approach cannot work well. For example, we use a VPN network [6] and malware bot networks may reject traffic from VPN networks. Second, they may monitor activity pattern. In fact, the recent version of Raccoon stealer detects unusual activity patterns [7]. To mitigate this type of side-effect, it is necessary to have a dirty IP address pool for this purpose, rotating them frequently and sending dummy requests to the C2 servers modestly.

We revealed that an AZORult user used Raccoon to spread the same additional payloads. In order to spread malware on a wide scale, attackers use several bot networks at the same time and we realized this characteristic is not limited to AZORult and Raccoon. For example, Amadey and Redline also showed similar activity [8]. Based on the findings, we guess other malware users will show similar behaviours in the other bot networks. While we used an emulator-based approach on this occasion, we can also use OSINT information to collect this type of information. This information is valuable for identifying attackers' behavioural patterns and potentially leading to attribution.

6. CONCLUSION

This paper provided the results of long-term analysis of AZORult C2 servers utilizing a malware emulator. The emulator scanned 2,364 C2 URLs since 27 January 2019 and collected 1,237 additional payloads samples. Overall, AZORult's activity is decreasing. However, an attacker used its bot network for 52 months. During this period, the attacker used the bot networks of both AZORult and Raccoon to spread the same malware samples.

This project yielded two important findings:

1. Even when a malware family's activity appears to be declining, attackers can still exploit the malware network for extended periods. Our findings demonstrate that attackers can sustain operations within these networks long after their peak activity has subsided.
2. An attacker can use different bot networks to spread the same malware at the same time. While there are challenges, it is valuable to monitor each malware family's activity over a long period, because it is useful to identify an attacker's behaviours and intent, and could potentially aid in attribution.

REFERENCES

[1] Proofpoint. Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan. July 2016. https://www.proofpoint.com/us/blog/threat-insight/threat-actors-using-legitimate-paypal-accounts-distribute-chthonic-banking.

[2] The BlackBerry Cylance Threat Research Team. Threat Spotlight: Analyzing AZORult Infostealer Malware. June 2019. https://blogs.blackberry.com/en/2019/06/threat-spotlight-analyzing-azorult-infostealer-malware.

[3] AhnLab Security Emergency Response Center. Infostealer Malware Azorult Being Distributed Through Spam Mails. August 2021. https://asec.ahnlab.com/en/26517/.

[4] AZORult Tracker. https://azorult-tracker.net/.

[5] Jaro-Winkler distance. https://en.wikipedia.org/wiki/Jaro–Winkler_distance.

[6] Private Internet Access. https://www.privateinternetaccess.com/.

[7] Llimos, N. A. Raccoon Stealer Announce Return After Hiatus. Cyberint. August 2023. https://cyberint.com/blog/financial-services/raccoon-stealer/.

[8] Kasuya, M. A Study on Long-Term Trends about Amadey C2 Infrastructure. JSAC 2024. January 2024. https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_1_kasuya_en.pdf.