Into The Silent Night

Yuta Sawabe, Ryuichi Tanabe, Fumio Ozawa and Rintaro Koike
NTT Security Holdings

This paper was presented at Botconf 2022, Nantes, 26-29 April 2022, www.botconf.eu
It is published in the Journal on Cybercrime & Digital Investigations by CECyF, https://journal.cecyf.fr/ojs

Abstract

Since the birth of Zeus family malwares, they have been sharpening their edge. Zloader is one of the active variants among Zeus family malwares. In December 2019, Zloader revived as "Silent Night." It communicates with C&C servers using DGA (Domain Generation Algorithm), because changing C&C servers' domain names can bypass malware detection systems. As a result, it makes it easier to steal information from infected hosts. This study proposes a system that traces Zloader's C&C servers automatically. This system collects samples, analyzes configuration data, and calculates DGA domains. Moreover, the system collects log files that store information about the infected hosts on the attackers' servers. The system can not only generate threat intelligence about Zloader for SOC and CSIRT but also follow the trend of attack campaigns. Furthermore, we will discuss how attackers acquire the DGA domains tactically.

Keywords: Banking Trojan, Zloader, Botnet Tracking, System Development.

1 Introduction

In December 2019, Zloader came back as "Silent Night", and it has been used in various attack campaigns since then [1]. It has especially been used in two attack campaigns (PseudoGate [2] and Malsmoke [3]). These attack campaigns aim at users in Japan, Canada, and the U.S. to obtain banking-related information. Zloader connects to its C&C servers with HTTPS and domain names generated by DGA. Therefore, it is challenging to trace attack campaigns.

We developed a system that collects information about infected hosts from logs on Zloader's C&C server. To find the C&C servers, we collected Zloader samples and extracted their internal config data using several public services. We have been making use of the system since March 2021. This system observes all Zloader's C&C servers for various attack campaigns, and we know the Zloader infection scale of each campaign on a daily basis.

In this paper, we will share the characteristics of Zloader first. Then, we will introduce the Zloader investigation system in detail. Furthermore, we will discuss the results of resolving DGA domain names generated by our system in terms of the relation of attack campaigns and the acquisition rate of the domain name. SOC, CSIRT, and security researchers who research Zloader will be able to have a deeper understanding and take a countermeasure against them.

2 Summary of Zloader

2.1 Overview

Zloader is a variant of banking trojan Zeus. It downloads banking malware components and other modules from a C&C server, then starts malicious activity [4]. In November 2019, a new variant of Zloader "Silent Night" was found on an underground forum [1]. Silent Night has been used in several attack campaigns [4, 5, 6, 7, 8, 9].

Malsmoke is one of the attack campaigns to infect malwares via Exploit Kit, fake software distribution, and so on [3, 10]. Zloader (Silent Night) is one of the last stage malwares in that campaign.

2.2 Characteristics

Zloader has its config data called BaseConfig that other Zeus variants have as well [11]. BaseConfig contains information such as Botnet ID, Campaign ID, RC4 key, C&C servers' URLs, and so on (Table. 1). To download additional components, Zloader accesses a C&C

server using one of the URLs in BaseConfig. Furthermore, security researchers can make a blacklist for Zloader detection and get the picture of attacking groups and campaigns based on BaseConfig information. Hence, BaseConfig is one of the essential factors to detect Zloader infection.

Zloader contains another implementation to communicate with C&C servers. If Zloader cannot access the C&C servers written in a BaseConfig, it will intend to communicate to other C&C servers. The C&C servers' domain names will be generated by using its DGA. To generate those domain names, Zloader needs two parameters: generation date and RC4 key in the BaseConfig [1, 11].

Table 1: Main items in BaseConfig

Items	Counts
Botnet ID	1
Campaign ID	2
URLs of C&C servers	Up to 10
RC4 key for DGA	1

2.3 Contents on C&C servers

On Zloader's C&C servers, log files are placed under /logs directory. One of the log files "av.log" contains information about infected hosts. (e.g., hostname, IP address, and country) (Fig. 1). The attackers can know about the infected hosts from those logs.

```
[17:59:17 25-11-21]
SUSAN-PC_62935DBE403EFB6B 198.51.100.103 US

[18:02:39 25-11-21]
DESKTOP-PA4VJ30_496730740D667A85 203.0.113.193 CA

[18:06:05 25-11-21]
TOSHIBA_05D93D74BFE8D440 192.0.2.247 JP
```

Figure 1: Example of av.log

3 About our system

We developed a system to trace Zloader's C&C servers (Fig. 3). Our system processes the following four steps to observe the Zloader's infection situation.

3.1 Collect malware samples

First, our system collects Zloader samples. At this time, we obtained the samples from the malware sample sharing services (VirusTotal [12], ANY.RUN [13], and MalwareBazaar [14]). It searches for the latest malware samples based on the tags of the malware family name (Zloader) to obtain the samples efficiently.

3.2 Extract BaseConfig

Next, our system extracts BaseConfig from the collected samples. To extract BaseConfig, we utilize an online sandbox service Triage [15]. Triage provides a service to extract config files from uploaded malware samples. This extraction will be automatically completed after uploading. By using Triage, we can automatically get BaseConfig information from the uploaded samples. (Fig. 2).

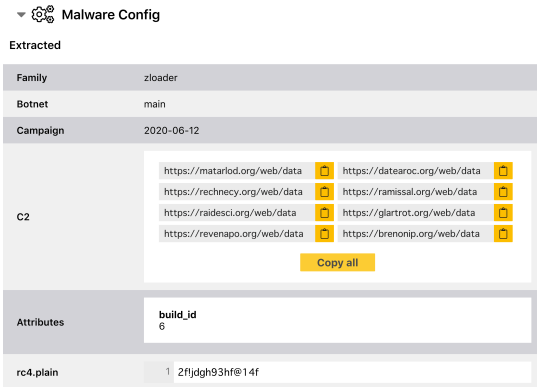

Figure 2: Extracted BaseConfig

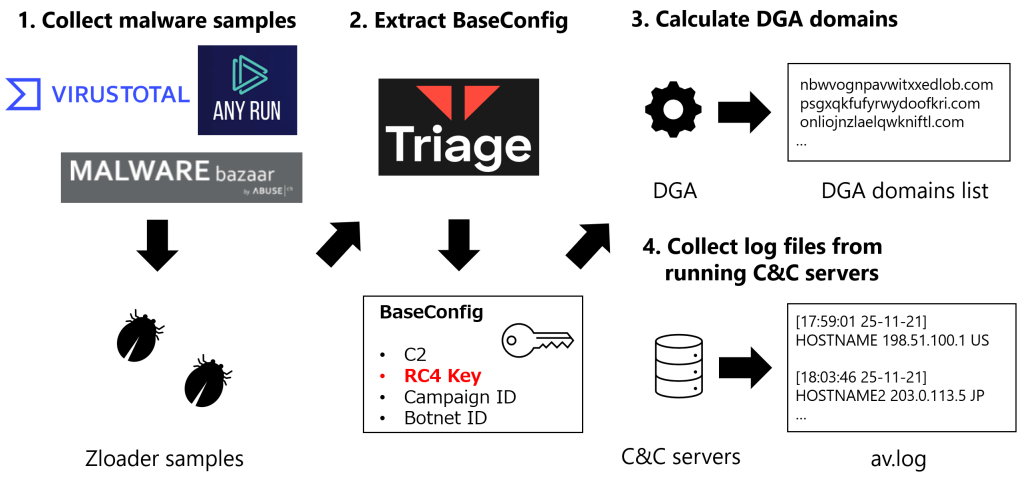

Figure 3: Overview of the system

3.3 Calculate DGA domains

Then, our system calculates DGA domains. As we mentioned in characteristics of Zloader section, if Zloader fails to connect to C&C servers written in BaseConfig, it will communicate with the domains generated by DGA. Fig. 4 indicates the algorithm to calculate the domains. The DGA used by Zloader contains the following characteristics:

- Using a date and an RC4 key for input value.
- Generated 32 domains by a date and an RC4 key.
- Using randomized 20 characters alphabet string for the domains
- TLD is '.com'

Our system can cover the DGA domains by calculating all the collected RC4 keys in the previous step.

```
def dga_calc(date_t, enc_key):
  dga_domains = []
  domain = struct.pack("<I", date_t)
  cipher = ARC4.new(enc_key)
  domain = cipher.encrypt(domain)
  pt = struct.unpack("<I", domain)
  pt1 = pt2 = pt[0]

  for _ in range(32):
      random_str = ""
      for _ in range(20):
          char = ord("a") + abs(pt1 % 25)
          random_str += chr(char)
          pt1 += char
          pt1 = (pt1 & 0xffffffff) ^ pt2
      dga_domains.append(random_str + ".com")
    return dga_domains
```

Figure 4: DGA calculation code

3.4 Collect log files from running C&C servers

Finally, the system collects av.log from each running C&C server.

Our system can cover the latest C&C servers' domains not only by extracting URLs from BaseConfig data but also by calculating DGA domains. In other words, it catches up with these domains. Therefore it generates threat intelligence about Zloader for SOC and CSIRT. Furthermore, it tells us Zloader's infection situation for each campaign from av.log files on the servers, hence we can automatically specify their latest trend as needed.

4 Result

We analyzed 453 samples using our system and obtained 22 RC4 keys. With the obtained keys, we calculated the DGA domains. As we mentioned before, Zloader calculates 32 domains per RC4 key. Therefore, we can extract 704 domains (32 domains $\times$ 22 keys = 704) per day in total. Furthermore, we have collected av.log files and counted the number of the infected hosts for six months since 1st March 2021 (Fig. 5). We can see that the number of infected hosts intentionally increased in September 2021. In the same period, a new attack chain to infect Zloader via fake-installers was reported [4]. It is thought that the appearance of this attack chain affected the increase of the infected hosts.

Table. 2 shows the number of infected hosts by country. The majority number of the infected hosts were in the U.S during the observation period. However, according to the results, the infected hosts from other countries were observed worldwide.

Table 2: Zloader infection rate by country

Country Name	Rate of Infected Hosts (%)
United States	90.7
Canada	3.1
Japan	3.1
Australia	1.5
United Kingdom	0.4
Netherlands	0.3
Turkey	0.2
Others	0.7

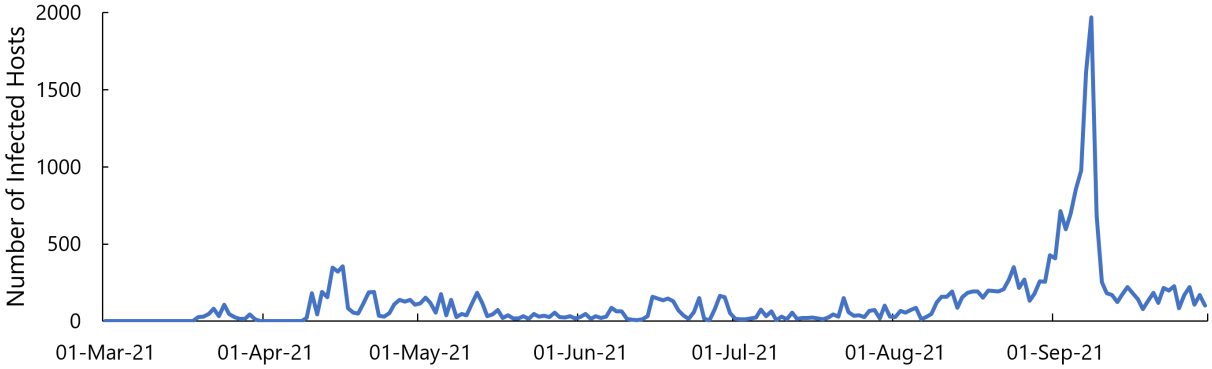

Figure 5: Number of Zloader infected hosts

5 Case Study

In this section, we will discuss the generated DGA domains using our system. It generates a lot of DGA domains based on dates and RC4 keys. However, the attackers do not obtain all the generated domains. Hence, we investigated the relation between the domain acquisition rate and the attackers' activities.

We investigated whether we could solve the generated domain names on 30th September, 2021. As we explained, calculating DGA domain names needs two input values: Date and RC4 key. We used 22 RC4 keys extracted from the collected Zloader samples by our system. About the dates, we set 90 days as an investigation period. We divided this period into two parts: X.) Past 60 days from the investigation date (2nd August. 2021 – 30th September. 2021), Y.) Until 30 days later from the investigation date (1st October. 2021 – 30th October. 2021).

5.1 Relation between threat activities and the RC4 keys

As a result of resolving the generated DGA domain names by using 22 RC4 keys, we found that eight keys could generate the DGA domains that could resolve at least one IP address (Table. 3). We assume that the C&C servers, which were related to those samples, may have already been stopped, because a part of our samples was old. It is known that a mutual RC4 key is used by each attacker or attack campaign. This means that resolving generated domain names can check whether an attacker or an attack campaign is active or not.

Table 3: RC4 keys used by DGA domains that successfully resolved

RC4 key	Value
A	03d5ae30a0bd934a23b6a7f0756aa504
B	41997b4a729e1a0175208305170752dd
C	2f!jdgh93hf@14f
D	q23Cud3xsNf3
E	e858071ef441a9a66f1a0506fc20b8c3
F	dh8f3@3hdf#hsf23
G	s4sd!@dss2QW11sdsdsa
H	kZieCw23gffpe43Sd

5.2 Correlation between RC4 keys

As mentioned in the previous section, an RC4 key can relate to an attacker or an attack campaign. However, an IP address binds to DGA domains generated by different RC4 keys in some cases. Our Zloader samples, which use the different RC4 keys (key "B" and "C" in Table. 3), do not have the same Botnet ID nor Campaign ID in the BaseConfigs. Hence, it would be decided that these samples had been used by different attackers. However, 100% of B's domains and 96.6% of C's domains were linked with the same IP address in our investigation period. This indicates that the samples, which have different RC4 keys, use a mutual platform. From these results, it can be assumed that the same attack group has used these malwares. This case study indicates that the result of the system can gather attackers' information that is not obtained from only malware analysis.

5.3 Timeline based domain acquisition rate

The most successfully resolved DGA domains were generated by RC4 key "A" during the entire investigation period (Table. 4). This key was used in Malsmoke campaign, and Malsmoke campaign had been active during that period. It can be said that there is a relationship between an RC4 key in BaseConfig and an attack campaign. On the other hand, as shown in Table. 4„ it is determined that attackers had obtained domain names that were used not only before but also after the investigation date. Although the acquisition rate of DGA domains after the investigation date was not very high, some DGA domains generated by RC4 key "A" were successfully resolved even one month later. This indicates that the attackers tend to get the DGA domains in advance and prepare a resolvable environment. Therefore, resolving the DGA domain names that will be used in the future can trace the future activity of a particular attack campaign.

Table 4: Domain acquisition rate focused on the timeline

RC4 key	Domain Acquisition Rate (%)		
	Past and Present (X)	Future (Y)	Entire (X+Y)
A	85.0	46.7	72.2
B	83.3	13.3	60.0
C	10.0	20.0	13.3
D	26.7	33.3	28.9
E	10.0	16.7	12.2
F	10.0	6.7	8.9
G	1.7	3.3	2.2
H	1.7	0	1.1

5.4 Generation order based domain acquisition rate

As written in the "Calculate DGA domains" section, Zloader calculates 32 DGA domains per day. If Zloader cannot access a C&C server using a generated DGA domain, it will attempt to use the next generated DGA domain in sequence. When we focused on the acquisition rate based on the order of DGA domain generation, we found that most of the first, second, and third DGA domains generated by each RC4 key could successfully resolve IP addresses. The rest of the generated domain could be rarely resolved (Table. 5). This

means that the attackers used only a part of the generated DGA domains, and the acquisition rate was biased. From these results, we assume that acquiring only a few domain names is cost-effective for attackers. These results can also be used for SOC and CSIRT to optimize their blacklist management. For example, if they register all of the calculated domains to their blacklist, they must prepare large storage for the blacklist because the number of the domains is too large. However, if they only register until third generated domains, the storage issue will resolve without decreasing the detection rate of Zloader infection.

Table 5: Domain acquisition rate focused on the DGA generation order
(n= the number of generated domain orders)

RC4 key	Domain Acquisition Rate (%)			
	n = 1	n = 2	n = 3	n = 4 – 32 (Min.–Max.)
A	72.2	50	8.9	0 – 2.2
B	70	5.6	1.1	0
C	13.3	0	1.1	0
D	28.9	2.2	0	0
E	5.6	1.1	3.3	0 – 4.4
F	8.9	0	0	0
G	2.2	0	0	0
H	1.1	0	0	0

6 Conclusion

This study proposed a system that automatically traces Zloader's C&C servers. This system collects samples, analyzes their configuration data, and calculates DGA domains that will be used after infection. This system can catch attackers' platforms even if new Zloader samples appear or C&C servers' IP addresses change. In addition, we can check the attack trend to collect the log files about the infected hosts from the attackers' servers. We investigated whether the DGA domains collected by our system could be resolved or not. We discussed the result showed that the acquisition rate of the domain name was biased. From these results, we discussed that it is possible to predict the trend of attack campaigns and the effective way to manage blacklist.

Author details

Yuta Sawabe

Yuta Sawabe is a SOC analyst at NTT Security Holdings. He received his B.E., M.E degrees in computer science from Waseda University in 2017 and 2019. Since joining NTT Communications Corporation in 2019, he has been engaged in SOC operation and malware analysis. He won the Specially Selected Paper Award from IPSJ (Information Processing Society of Japan).

Ryuichi Tanabe

Ryuichi Tanabe is a SOC analyst at NTT Security Holdings. Currently, his main duty is responding to EDR detection, but he also works as a malware analysis researcher. Now his interest is malware families related to APT attacks targeting East Asia. Previously he worked as a web programmer, but he changed his career to become a SOC engineer in 2012. Since then, he has specialized in SOC related works. He has been a speaker at VB, SAS and CodeBlue.

Fumio Ozawa

Fumio Ozawa is a security analyst at NTT Security Holdings, where he runs malware and exploit analysis, and the SOC operation. Recently he has focused on analyzing APT attacks to East Asia. He has spoken at JSAC 2018 and VB 2020, and has written several white papers.

Rintaro Koike

Rintaro Koike is a security researcher at NTT Security Holdings. He is engaged in threat research and malware analysis. In addition, he is the founder of "nao_sec". He focuses on APT attacks targeting East Asia and web-based attacks. He has been a speaker at VB, SAS, Black Hat USA Arsenal and others.

References

[1] Malwarebytes, "The "Silent Night" Zloader/Zbot." https://www.malwarebytes.com/resources/files/2020/05/the-silent-night-zloader-zbot_final.pdf.

[2] NTT Security Holdings, "Attack using Spelevo Exploit Kit by PseudoGate campaign targeting Japan." https://insight-jp.nttsecurity.com/post/102gsqj/pseudogatespelevo-exploit-kit.

[3] Malwarebytes Labs, "Malvertising campaigns come back in full swing." https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/.

[4] Sentinel Labs, "Hide and Seek | New Zloader Infection Chain Comes With Improved Stealth and Evasion Mechanisms." https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/.

[5] Trend Micro, "Zloader Campaigns at a Glance." https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zloader-campaigns-at-a-glance.

[6] K7 Security Labs, "Java Plug-Ins Delivering Zloader." https://labs.k7computing.com/index.php/java-plug-ins-delivering-zloader/.

[7] PhishLabs, "Surge in ZLoader Attacks Observed." https://www.phishlabs.com/blog/surge-in-zloader-attacks-observed/.

[8] McAfee, "Zloader With a New Infection Technique." https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/.

[9] Check Point Research, "Can You Trust a File's Digital Signature? New Zloader Campaign exploits Microsoft's Signature Verification putting users at risk." https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/.

[10] Malwarebytes Labs, "Malsmoke operators abandon exploit kits in favor of social engineering scheme." https://blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/.

[11] Proofpoint, "ZLoader Loads Again: New ZLoader Variant Returns." https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns.

[12] VirusTotal. https://virustotal.com.

[13] ANY.RUN. https://any.run.

[14] MalwareBazaar. https://bazaar.abuse.ch.

[15] Hatching Triage. https://tria.ge.