LokiBot – Phishing Malware Baseline

Archived: 2026-04-05 18:41:20 UTC

By Madalynn Carr Report

LokiBot is an Information Stealer with expanding capabilities depending on the threat actor. This malware family was originally written in C++ and targets Windows devices. LokiBot was first advertised in 2015 on underground markets in Eastern Europe, however it was not common to see it in the wild until 2018. Since then, LokiBot has remained in the top five malware families delivered through phishing emails.

History

LokiBot first surfaced in March of 2015 on underground hacking forums by a hacker with an alias of “lokistov”, who is also known as “Carter”. This can be seen in Figure 1, where LokiBot was originally posted on an underground form. LokiBot was originally advertised as a “Resident Loader and Password and CryptoCoin-wallet stealer.” It is assumed that lokistov is from a non-English speaking country, specifically an ex-USSR country. LokiBot was being sold for upwards of $450 USD or $540 USD in the current economy this report was written, depending on whether the buyer wanted the stealer or the loader, as well as other add-ons such as a change in the C2 (Command and Control) IP address. After release, every week lokistov would publish an update until 2017, when lokistov released LokiBot V2. Since then, they have not updated the forums for LokiBot V1. Shortly after, the LokiBot source code was leaked around 2018 and is now being sold on forums for as low as $80 USD. There are two theories of how this happened. One is that somebody reversed the original LokiBot and gathered the source code, then published the cracked version of the malware. The other theory is that lokistov got hacked themselves, and the hacker published the stolen version.

Figure 1: Original Posting of LokiBot by Lokistov.

LokiBot became a popular malware choice for threat actors due to the low price and ease of use. Since then, lokistov has released LokiBot 2.0 and is currently selling it on underground forums. This newer version of the Information Stealer includes more evasive techniques and expands further into Keylogger, Remote Access Trojan (RAT), and even ransomware attributes.

Notable Uses

Due to LokiBot being around for a while, there have been a sizeable number of media pieces revolving around LokiBot, however none of them revolve around the campaigns that APT (Advanced Persistence Threat) groups are using this malware to conduct. The most recent use was in February of 2020, where LokiBot impersonated a Fortnite launcher, which was one of the most popular video games at the time. Since LokiBot is simple, adaptable and easily accessible, this malware has remained in the top 5 malware families seen at Cofense since 2019. During 2019 and 2020, LokiBot was a high competitor for the top malware family seen, constantly switching places with the ever-popular Agent Tesla.

Capabilities

Although LokiBot originated as an Information Stealer, it has been cracked and edited several times. LokiBot can have RAT or keylogger capabilities. However, the majority of LokiBot seen in the wild only demonstrates Information Stealer capabilities. LokiBot is capable of stealing credentials from over 100 different clients, including but not limited to:

- Email Clients
- FTP Clients
- VNC Clients
- HTTP Browsers
- Password Managers
- IM Clients

Specific examples of what these applications are can be found in Table 1, however the list is not limited to just these specific applications.

Mozilla Firefox	Internet Explorer	Google Chrome	K-Meleon	Comodo Dragon
SeaMonkey	Safari	CoolNovo	Opera	Chromium
Titan Browser	Yandex Browser	Superbird Browser	Chrome Canary	Waterfox
Flash FXP	Nexus File	JaSFtp	Syncovery	Remmia RDP
FileZila	CyberDuck	NovaFTP	FTPShell	NETFile
mSecure Wallet	Fling	KiTTY	PuTTY	WinSCP
Outlook	Mozilla Thunderbird	Pocomail	Gmail Notifier Pro	yMail
Pidgin	AI RoboForm	KeePass	EnPass	1Password

Table 1: List of examples that LokiBot has the capability to steal from.

In the Wild

LokiBot has always been seen at Cofense as one of the most popular malware families used by threat actors. Due to its simplistic nature and usage, low-skill threat actors can use LokiBot for a variety of malicious purposes. In

2019 up until around 2021, LokiBot would often be the most common malware family, followed by Agent Tesla Keylogger. At the time of this report, other malware families have appeared more often, and therefore pushed LokiBot down in the rankings. However, LokiBot is still in the top five malware families seen at Cofense. Figure 2 shows the percentage of LokiBot malware seen among other malware families in our Active Threat Reports (ATR), and although there was a small dip over the past year and a half, LokiBot has remained around eight percent of all malware seen each month.

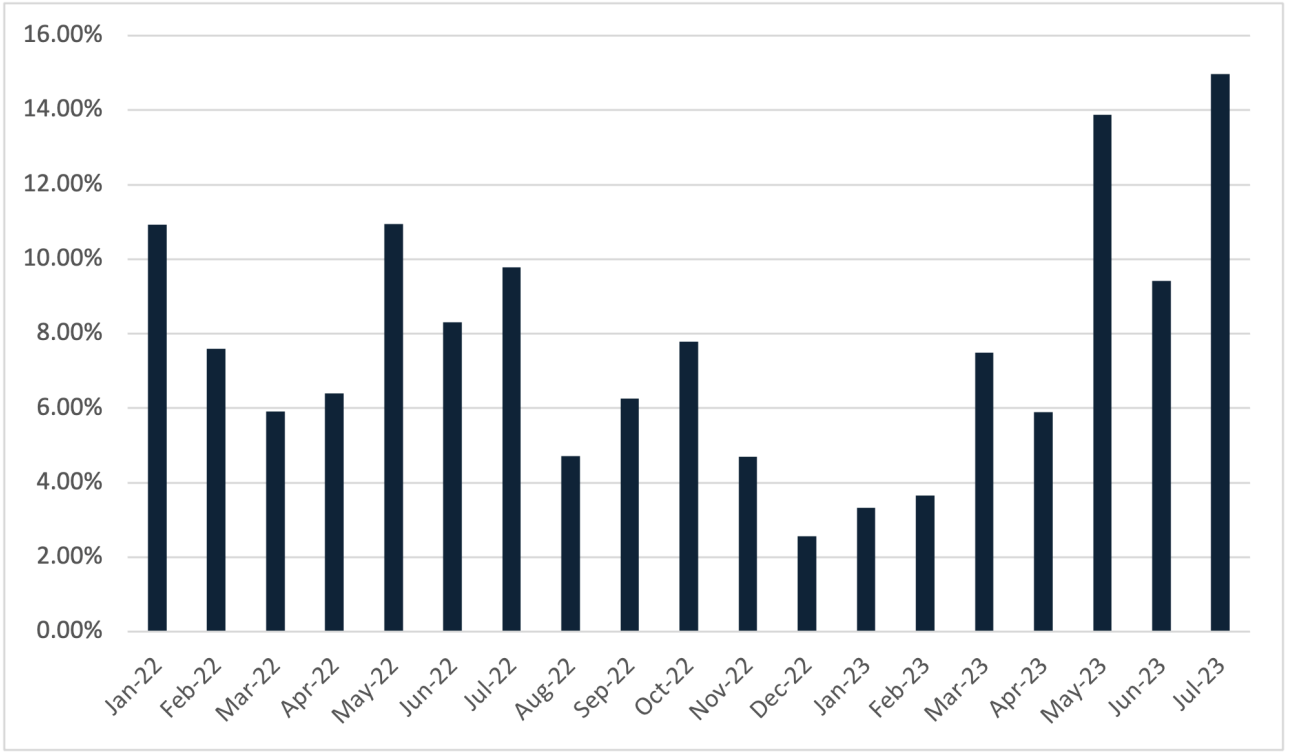

Figure 2: Loki Bot's relative value seen at Cofense between January 2022 and July 2023.

Delivery Mechanisms

LokiBot is often seen by itself when it is delivered via email, however, as can be seen in Figure 2, there is still quite a large amount of LokiBot that is accompanied by a delivery mechanism. Out of the delivery mechanisms seen by Cofense, an overwhelming 82% of LokiBot accompanied by a delivery mechanism is delivered by CVE-2017-11882. However, out of all the LokiBot samples seen by Cofense, over half of the LokiBots are seen delivered as a direct attachment.

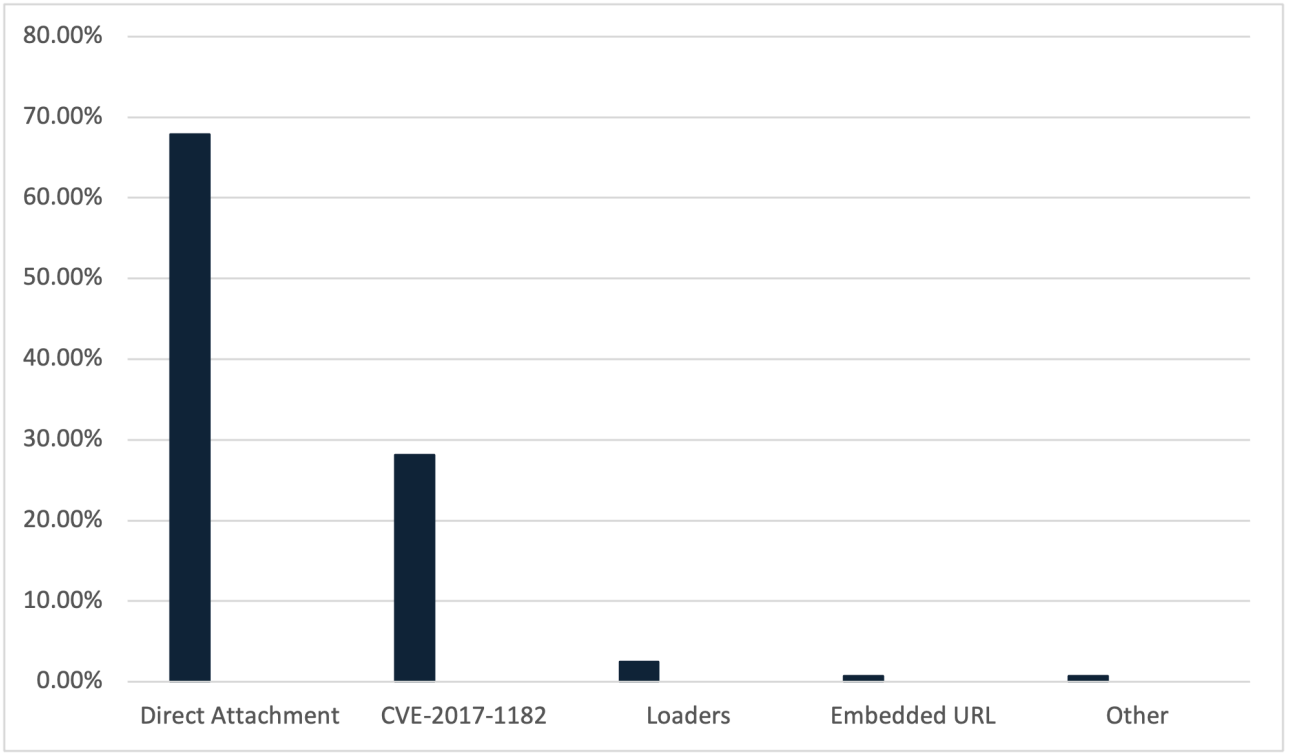

Figure 3: Delivery Mechanisms used to deliver Loki Bot between January 2022 and July 2023.

Very rarely will LokiBot be delivered via embedded URLs or other forms of delivery mechanisms except for CVE-2017-11882, such as Visual Basic Scripts (VBS) or Windows Shortcut File (LNK), as just over one percent of LokiBot samples were seen to be delivered via both delivery mechanisms combined between January 2022 to July 2023.

Behavior

LokiBot has a very straightforward and simplistic way of behaving. Once LokiBot has been downloaded and run, LokiBot will unpack itself onto the system. From there, this malware will start collecting sensitive information from each of the programs it supports gathering information from. Once LokiBot has exhausted all the possible applications that can give the sensitive data, as well as any extra additions such as keystroke logging, it will create a customized HTTP packet and send it to the C2, as seen in Figure 4. As LokiBot is gathering the information into an HTTP packet, some versions of LokiBot will start to maintain persistence, while others may continue to run and occasionally connect in case any new credentials are stored on the machine.

```
POST /chandler/five/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 194.55.224.11
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 400A33A6
Content-Length: 197
Connection: close
```

Figure 4: Example of an HTTP POST request from a computer infected with LokiBot.

This specific link is the final destination, where the information is presented to the threat actor. If one were to visit the page, they would be greeted with a captcha as well as a login page as seen in Figure 5.

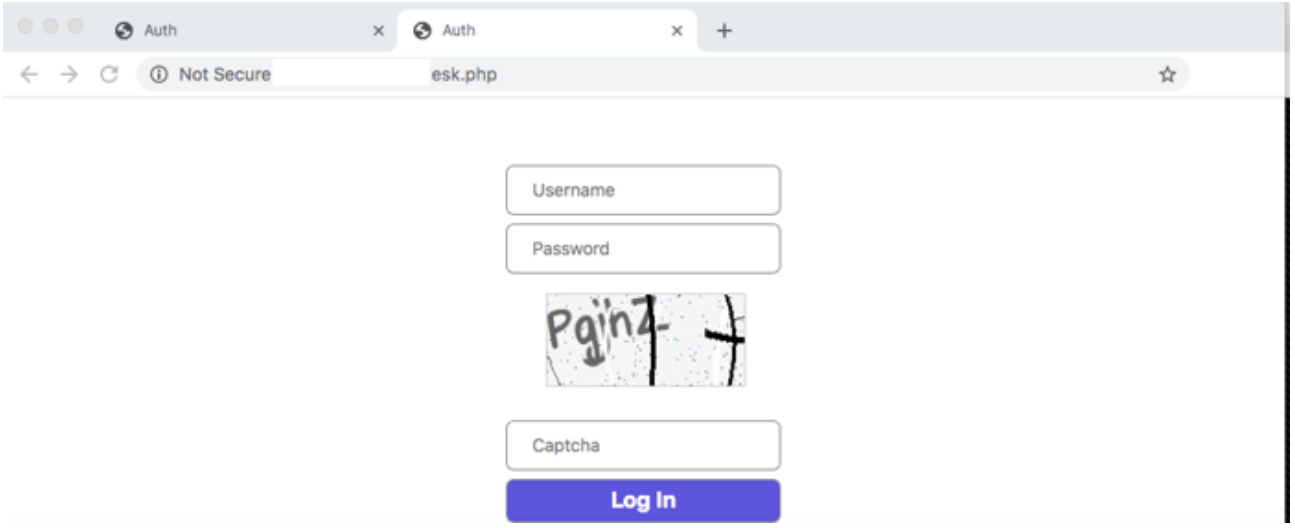

Figure 5: Example of a LokiBot C2 Authentication Panel.

Detection and Hunting

LokiBot heavily depends on connecting to its C2, and therefore makes detection generally easy to spot. Due to the low volume of embedded URLs delivering LokiBot, the primary way to prevent LokiBot from being installed on a system is to not allow unknown downloads from suspicious emails. Most anti-virus software is good at catching LokiBot due to its simplicity, but there are also other ways to spot if LokiBot is already installed on a system.

User Agent

LokiBot can also be identified by a specific string found in the application as well as the network traffic. LokiBot will always use the User Agent “Mozilla/4.08 (Charon; Inferno)” to connect to its C2s, as seen in Figure 4.

Network Traffic

As previously mentioned, LokiBot will use the User Agent “Mozilla/4.08 (Charon; Inferno)” to post the credentials to its C2 Panel. LokiBot primarily only uses HTTP to communicate to its C2. There are a variety of ways the URL can be formatted, but the file that the link is accessing is typically followed by a PHP panel or ends with a “p=” followed by a unique set of numbers to differentiate the systems that LokiBot has infected. An example of this that Cofense has previously reported is: “hxxp[://]216[.]128[.]145[.]196/~wellseconds/?p=” A more common example is the other IOC mentioned, which is the PHP panel whose URL looks similar to: “hxxp[://]194[.]55[.]224[.]9/fresh1/five/fre[.]php”.

fre.php	gate.php	aaaj.php	nimda.php	ight.php	crkk.php
free.php	wish.php	base.php	fred.php	mono.php	mime.php

Table 3: Examples of PHP Panels that have been seen as a C2 for Loki Bot.

The examples listed in Table 3 are not an exhaustive list of all panel PHPs as LokiBot can change the name of the PHP panel. However, the majority of LokiBot will use “fre.php” when connecting to its host.
