PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

RIG Exploit Kit
In-Depth Analysis

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

Reference Number	CH-2023012301
Prepared By	PTI Team
Investigation Date	14.09.2021 - 27.09.2021
Initial Report Date	19.10.2021
Last Update	27.02.2023

1 Introduction

Exploit kits (EK) are typically used to distribute malware and other malicious programs to large numbers of victims using existing vulnerabilities in commonly-used browsers. Once a user visits the exploit kit's web page (landing page), multiple techniques are used to identify the browser version and operating system. With this information, the system picks a suitable exploit that might allow for command execution on the victim's device. Subsequently, this action is, in most cases, used to install malware on the computer.

This report explores information related to the victim statistics, operation, C&C server, and technical aspects of one of the well-known exploit kits, **RIG EK**. Most notably, the RIG EK manages the software distributing exploits and collecting victim data in their control panel called **RKIT**. This name can be seen in the HTML page's title and occurs in the control panel's top-left.

Many reputable sources have already provided valuable analysis into the inner workings of the RIG EK and taken action against them via organized take-downs of their landing pages. However, RIG has recently resurfaced and continues to distribute malware to hundreds of victims daily.

RIG EK is a financially-motivated program that has been active since 2014. Although it has yet to substantially change its exploits in its more recent activity, the type and version of the malware they distribute constantly change. The frequency of updating samples ranges from weekly to daily updates.

In general, this report aims to provide insight into how RIG EK operates, what kinds of malware it distributes, and how the distribution happens. The PTI team has identified and gained visibility of the control panel of RKIT, which revealed threat actors' inner workings and identities.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing the global fight against high-end threat actors and APTs.

2 Executive Summary

Even though we like to think that the amount of machines running software with 0-day vulnerabilities has significantly declined in the past decade - thanks to rolling security updates and better security research - that is, sadly, not the case. There still remains a considerable amount of machines worldwide running outdated and vulnerable software - especially Internet Explorer.

RIG EK uses this untapped goldmine by exploiting machines that run outdated versions of Internet Explorer. Threat actors pay the RIG EK administrator to install their malware on victim machines. So far, this has proven to be a very profitable business model for the RIG administrator and the threat actors.

The operators of the RIG mainly use malvertising to ensure a high infection rate and worldwide coverage. Victims' initial infection occurs when they visit a site that has been compromised or when they visit an advertising page that RIG EK controls. Once they access the landing page, the site determines whether the browser is vulnerable. If not, the user remains unaffected. However, if a vulnerability is detected, they are then redirected to one of RIG's proxy servers which communicate with the exploit server that sends the exploit for that browser version.

Since the exploit server tracks every request sent to it and synchronizes the victim data with the C&C, the system stores the connection time, IP, OS, Browser version and information on whether exploitation was successful or not for each user. All of this allowed the PTI team to conduct an extensive analysis of the logged data.

The artful design of the Exploit Kit allows it to infect devices with little to no interaction from the end user. Meanwhile, its use of proxy servers makes infections harder to detect. These two features combined turn RIG EK a significant threat to corporations and end users.

RIG EK has been observed dropping multiple types of malware, including stealers, RAT, cryptocurrency miners, and banking malware. The C&C server allows for auto-updating the malware by providing a download URL. Because of this feature, the server samples get updated frequently, ranging from daily to weekly updates. Moreover, RIG EK also has an integrated Antivirus testing feature which controls for malicious software whether any popular antivirus software caught it.

One of the most prominent types of malware that RIG has been observed dropping is **Dridex**. After close inspection, it appears to be one of the most well-maintained malware with the most regular updates, with a new version being released daily. Moreover, when the PTI team analysed extensively, they observed that the RIG administrator had taken additional manual configuration steps to ensure that the malware was distributed smoothly. Considering all these facts, we assess with **high confidence** that the developer of Dridex malware has a close relationship with the RIG's admins.

3 The RIG Timeline

RIG is a very old exploit kit with a journey that went on for several years. Even though it went through several ups and downs, it is still going strong. A very general overview of what happened during its lifetime can be seen in **Figure 3**. In this section, we will be going over the key points in more detail.

3.1 First Release

RIG EK was initially released in 2014, on several forums. It promoted several exploits in its arsenal, including but not limited to **CVE-2012-0507**, **CVE-2013-0074**. The screenshot of an advertising forum post can be seen on **Figure 1**.

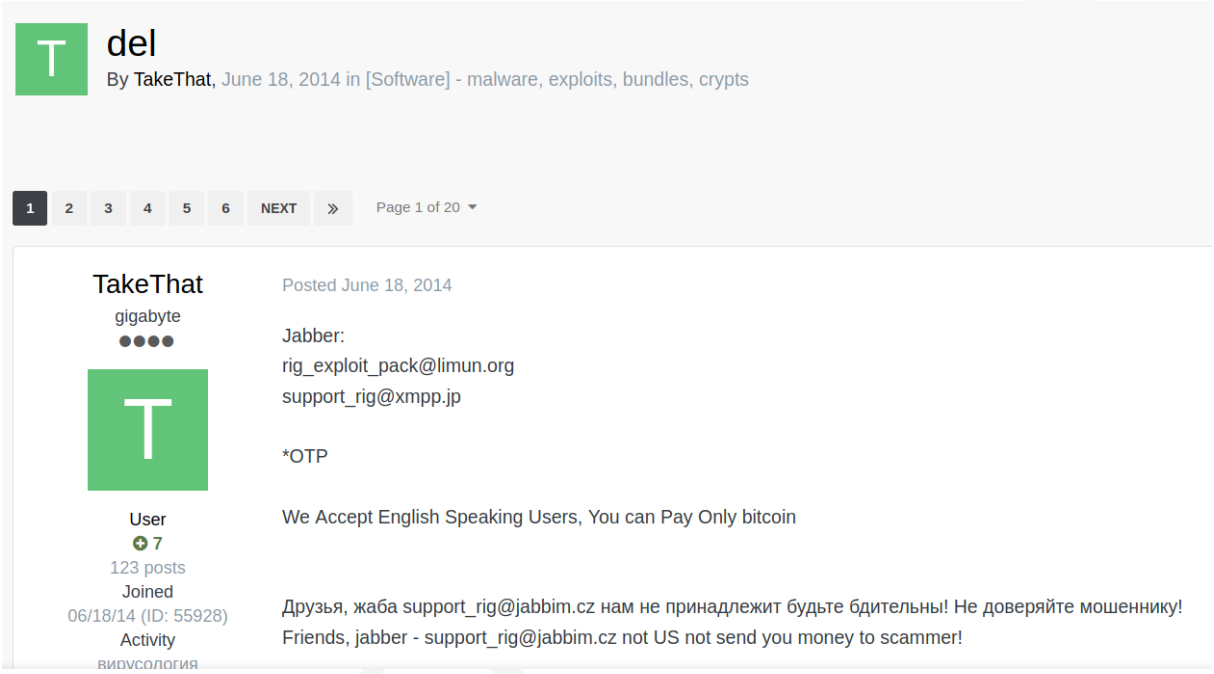

Figure 1. A forum post promoting RIG EK.

3.2 Takedown Operation

After operating for a year, its source code is leaked and started getting distributed across forums. Two years after this major blow, it got hit by **Operation Shadowfall**, a coordinated takedown operation organized by the RSA organization. [2] This led to RIG EK significantly downsizing its operations for a period of time.

3.3 A Change of Malware

During this time, RIG EK was mainly distributing **Racoon Stealer**. However, after the death of Raccoon's maintainer due to the Russian advances on Ukraine, it was forced to switch into distributing **Dridex** [4]. This was one of the main events that caused the PTI team to be interested in RIG EK.

A short while after continuing its operations despite this event, RIG EK's operator announces the shutdown of the kit on the very same forum it was announced. The post of the announcement can be found in **Figure 2**. It translates into "We are pausing our RIG3 operation for an indefinite amount of time."

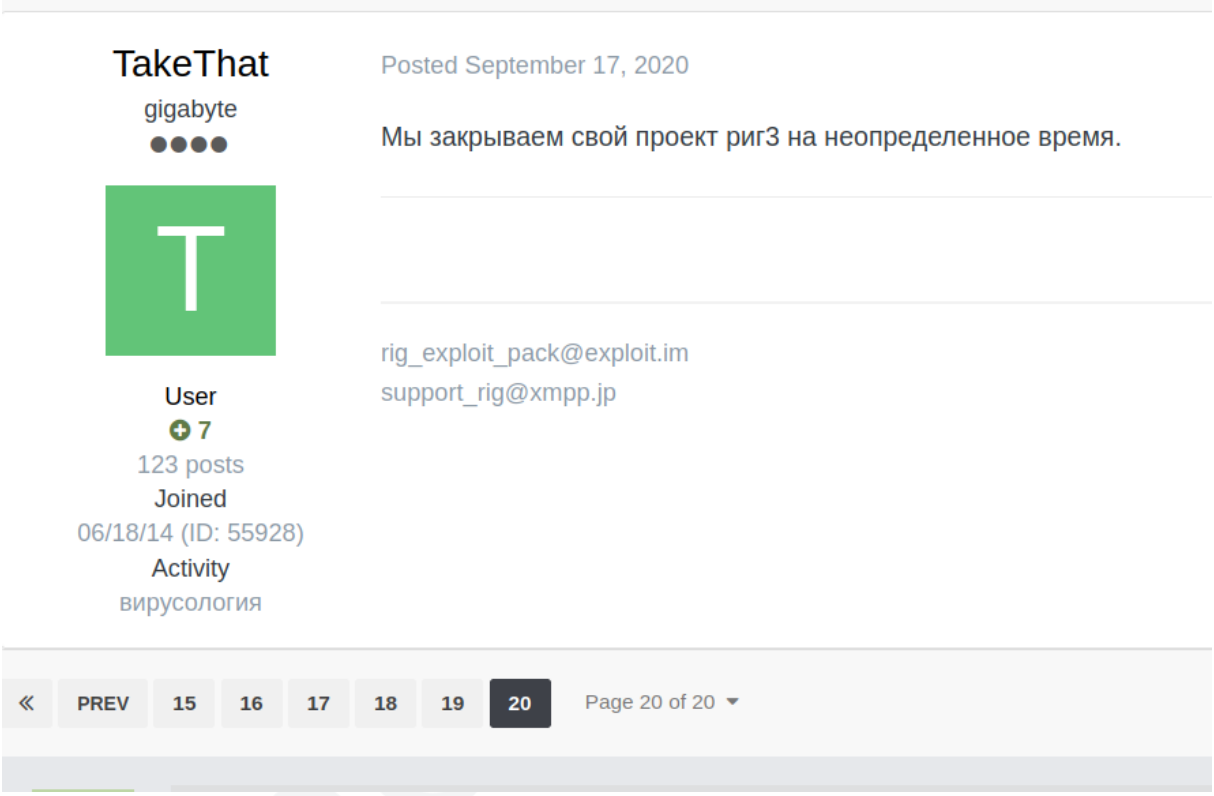

Figure 2. A forum post announcing RIG's shutdown.

3.4 Resurfacing

A year after the closing announcement, RIG EK resurfaces with a new and more modern set of exploits. The source code leak has raised some concerns among the PTI team on whether the person operating the RIG EK before and after the shutdown was the same person. Those concerns were addressed after the discovery that both new and old instances of the RIG EK uses the same VDS server. This conclusion was also supported by the connections. In the new RIG instance, the exploit kit was packing two shiny new exploits : **CVE-2021-26411** and **CVE-2020-0674**. With this new technical advance, its successful exploitation skyrocketed and reached an all time high of **30%** in 2022.

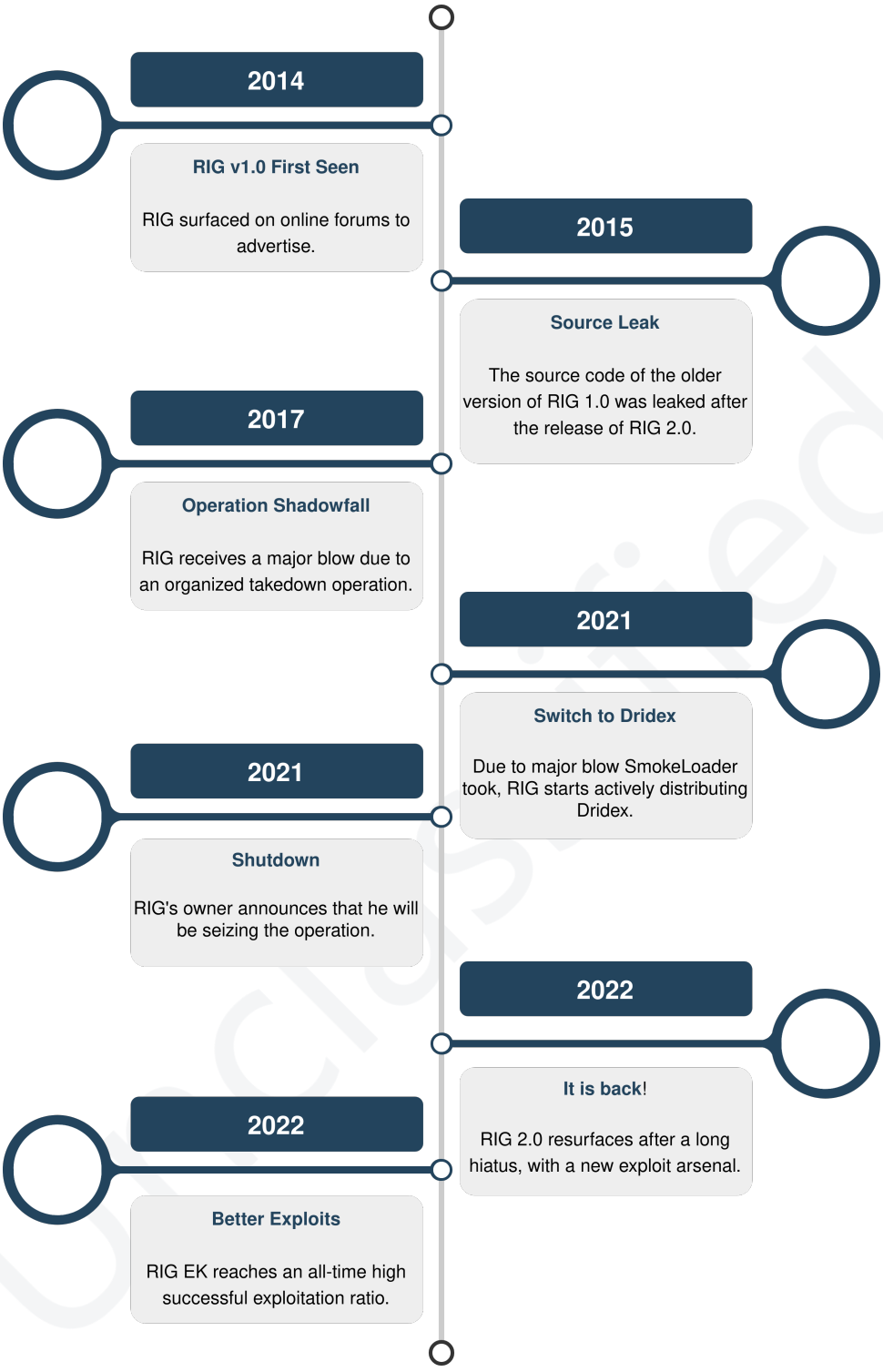

Figure 3. **A timeline of RIG pertaining to the most important points during its life.**

4 Technical Analysis

This section contains a technical analysis of the RIG Exploit Kit. Exploit kits are used for spreading malware by using predefined exploits. The RIG Exploit Kit is known as a dropper helping the spread of the malware [3] such as **RTM banking** malware [5], **Dridex** [4], **Raccoon Stealer** [6], **CryptoBit** ransomware [7], and **AZORult** malware [1] since 2014. Recently, it is used as a dropper for SmokeLoader and Ursnif.

4.1 Profiling

Since the main purpose of RIG EK is to gain access to victim computers and hand that access over to other threat actors, it makes use of **Resource Development**, **Initial Access** and **Execution** TTPs.

4.1.1 Resource Development

RIG EK uses already known vulnerabilities in browsers to execute commands in victim machines. The exploits used for these vulnerabilities do not appear to be custom developed by the RIG author or anyone else. Rather, they appear to be slightly modified versions of publicly available exploits, usually (but not always) obfuscated to hide the code. This behavior falls under the **T1588, Obtain Capabilities** [1] TTP. Moreover, RIG EK uses malvertising and compromised websites to redirect worthy users into its landing page. This correlates with the TTP **T1584, Compromise Infrastructure** [2].

4.1.2 Initial Access

The exploits of RIG EK are delivered to unsuspecting victims in two ways. Either via malvertising, where users are redirected to online advertising pages that are tricked to execute the RIG exploits on their browser. Or when they visit sites that were compromised and the exploit kit's javascript was injected. In either way, the users hardly every notice that anything malignant has ever occurred on their systems and go on with their daily browsing activities. Due to the very limited interaction and non-disrupting nature of this process, this technique can be deemed **T1189, Drive-by Compromise** [3].

4.1.3 Execution

After the exploit kit is successfully executed on the victim machine, it runs an obfuscated powershell script that fetches a malware from the RIG EK C&C infrastructure. This falls under the **T1059, Command and Scripting Interpreter** [4] TTP. Meanwhile, since the script was initially executed via the exploitation of a known vulnerability in the victim's system, it can be said that the TTP **T1203, Exploitation for Client Execution** [5] is also made use of by RIG EK.

1. https://attack.mitre.org/techniques/T1588/
2. https://attack.mitre.org/techniques/T1584/
3. https://attack.mitre.org/techniques/T1189/
4. https://attack.mitre.org/techniques/T1059/
5. https://attack.mitre.org/techniques/T1203/

4.2 C&C Infrastructure

The threat actors that maintain the RIG exploit kit modernized and changed their codebase but did not change their infrastructure [8] since their source leak in 2015. Also, it is discovered that they did not update their configuration constants like XOR keys and API keys.

The infrastructure had three keystones. These are the Virtual Dedicated Servers (VDS) (a.k.a. the exploitation server), the proxy server, and the API server. The API serves the exploit in an iframe or an under pop through the proxy server. (Figure 4)

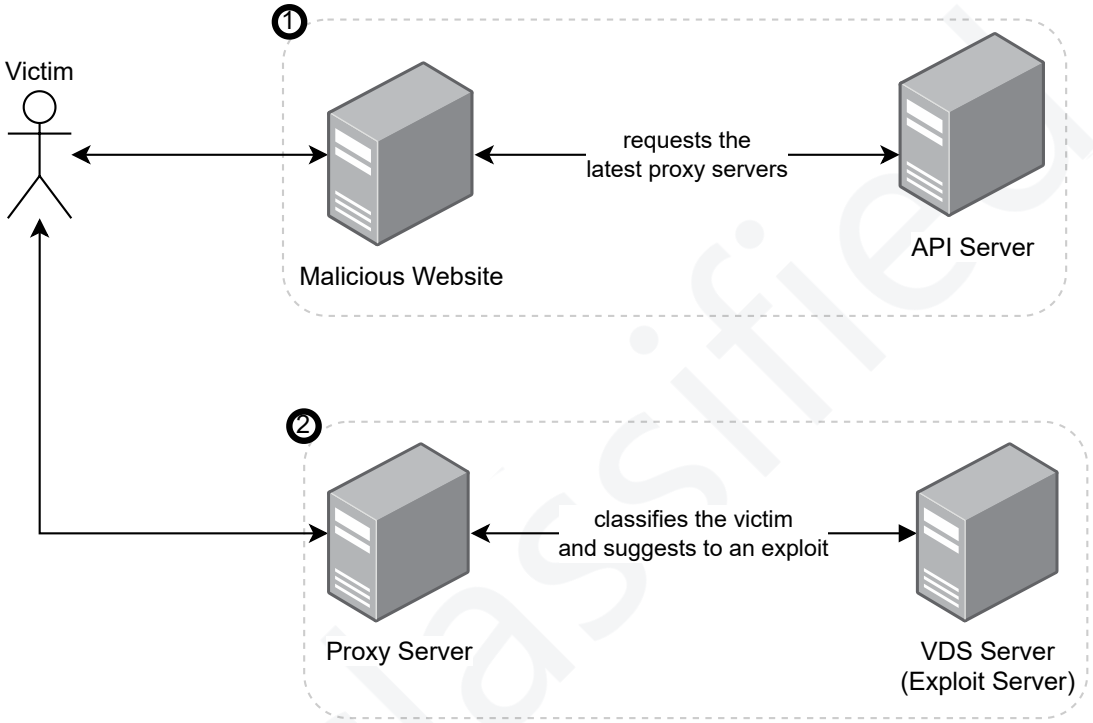

Figure 4. The infrastructure of the RIG exploit kit.

The proxy server is a reverse proxy to the exploit server. The proxy server uses a pre-shared protocol with the VDS. In that protocol, the first step is serializing the HTTP request with the referral site's information. Then it redirects the exploit server's response to the victim's browser. The referral sites information is stored for statistical presentation in the management panel.

The exploit server detects user's browser by parsing the "User-Agent" header. If the version of the browser matches the pre-defined vulnerable browser versions, then the exploit kit returns the suggested exploit code encrypted with custom version of RC4 algorithm.

The exploit server had six different exploits. Based on the PTI teams analysis, every exploit inside the RIG exploit kit, are weaponized versions of publicly available proof of concept (PoC) exploits codes. According to the exploit statistics, the actors are only using two of these exploits actively.

These exploits are :

- CVE-2013-2551
- CVE-2014-6332
- CVE-2015-0313
- CVE-2015-2419
- CVE-2016-0189
- CVE-2019-0752
- CVE-2018-8174

Since RIG EK has resurfaced, the group has expanded their arsenal with two new exploits that are used actively :

- CVE-2021-26411
- CVE-2020-0674

4.3 Management Panel

Multiple users use the management panel with various privilege levels. The PTI team monitored the management panel and its users cautiously, and the below table shows the active users and their respective roles in the system.

Username	Privilege
admin	admin
vipr	admin
pit/pitty	subadmin
lyr	user
ump	user
test1	user

Since the user **admin** is a dummy user used for creating other users, actors used the **pitty** user for managing the panel. The management panel works with a subscription model. The subscription of the only existing user, pitty, ended on the 5th of June, 2022. (as shown in Figure 5)

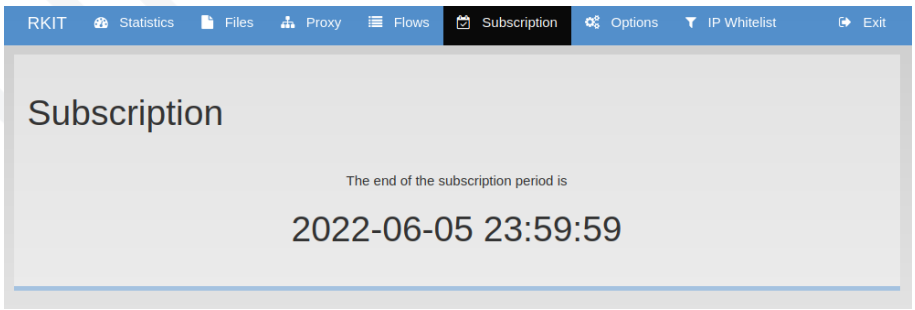

Figure 5. The actor pitty's subscription information.

The main page of the management panel shows the exploit kits statistics (as shown in Figure 6). The panel lets the actor filter the statistics by time, exploits, countries, browsers, the operating system, referrer websites, and the panel users.

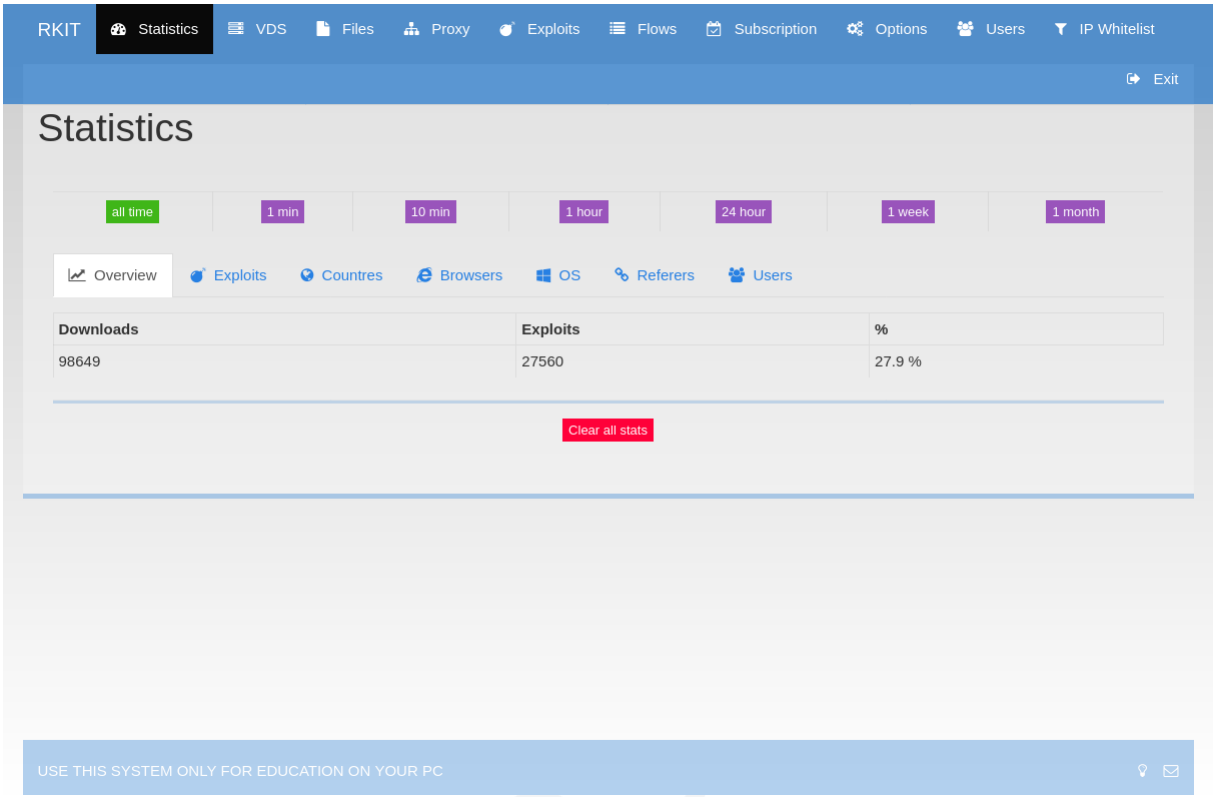

Figure 6. The management page welcomes the actor with the statistics page.

The panel lets its users run multiple flows (campaigns). Each flow had a revocable unique token (Figure 7). The tokens are used for identifying the flow when serving the relevant exploits to the victims. Some of the flow names found during the investigation are :

- DanFuz Buba TOP 43k
- DanFuz Buba
- TEST MAGMA RIG
- ZWhttp
- godf WW 10k
- DanFuz WW 42k
- ANKL JP

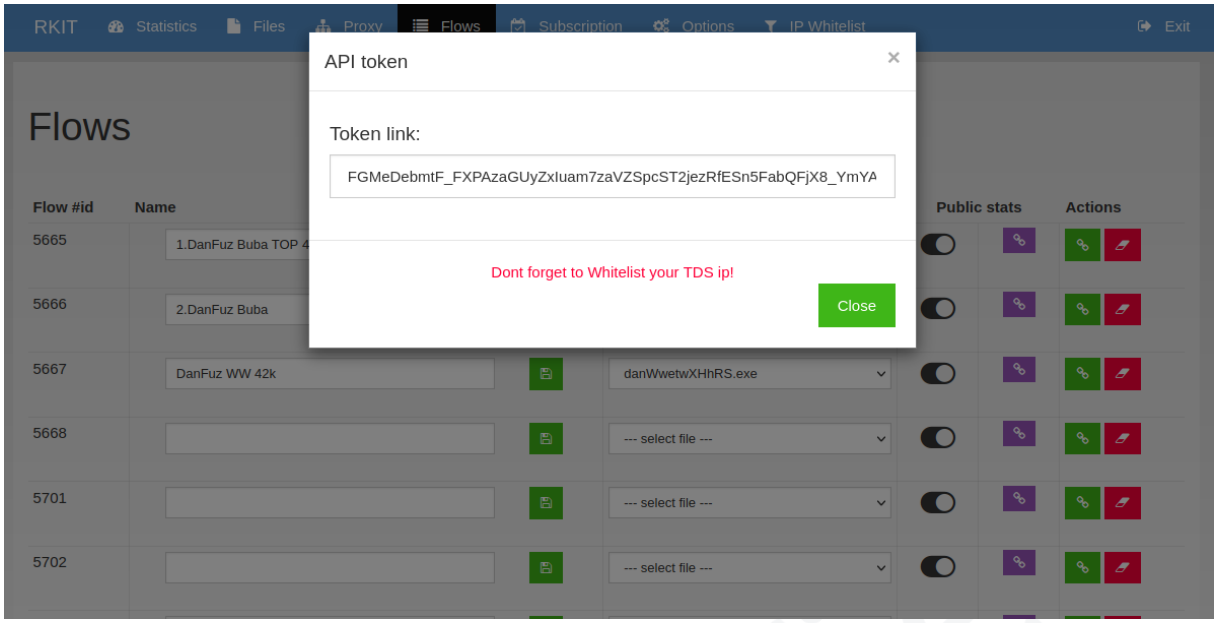

Figure 7. **A flow created by the threat actor and the flows key.**

The "Files" page on the panel allows uploading, managing, and scanning files. Files could be uploaded in two ways. First way is to upload files directly from a disk or an URL. The second way is to define an auto-update URL. With an auto-update URL, the panel will fetch the URL in intervals and update the file periodically (Figure 8).

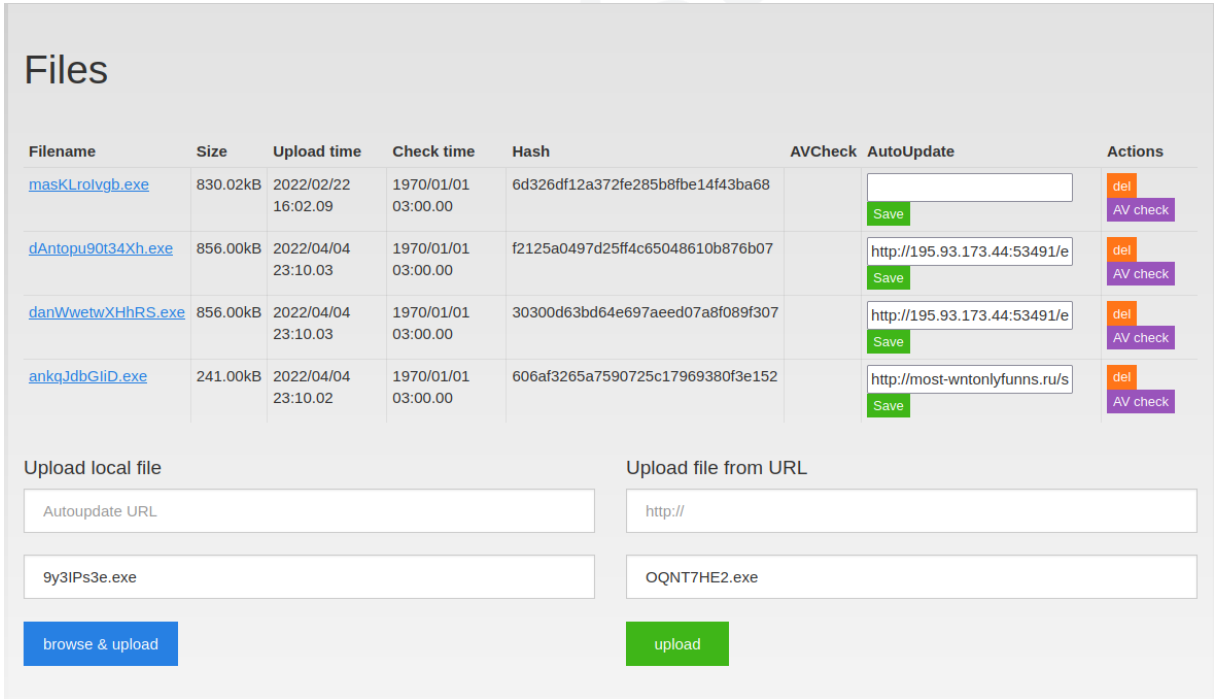

Figure 8. **The malware upload page of the system.**

The management panel allows managing the reverse proxies as well (Figure 9). These proxies are used for hiding the exploit server from being exposed to the public.

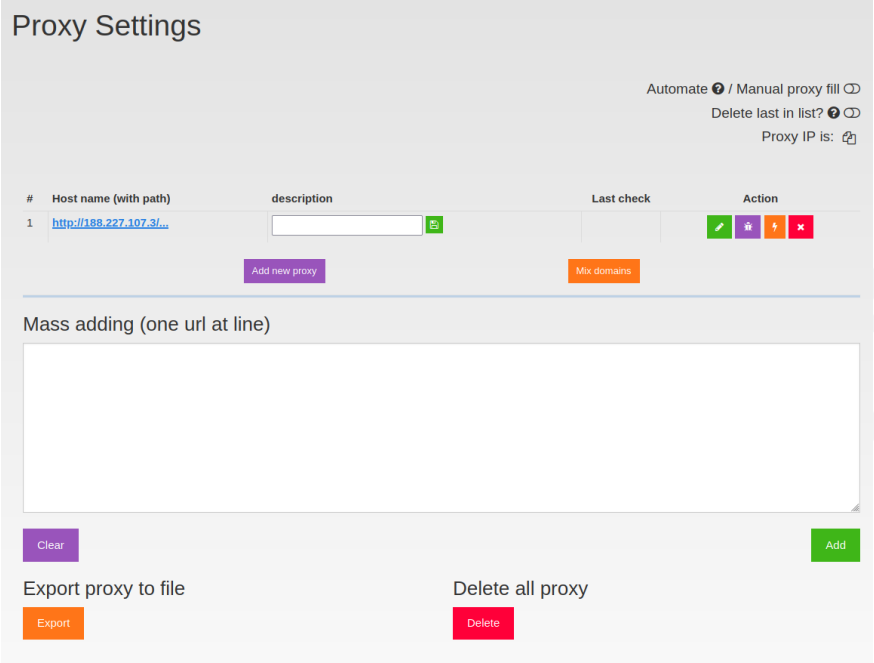

Figure 9. Proxy management page.

The panel allows the admin users to download the exploits from the exploit server (Figure 10).

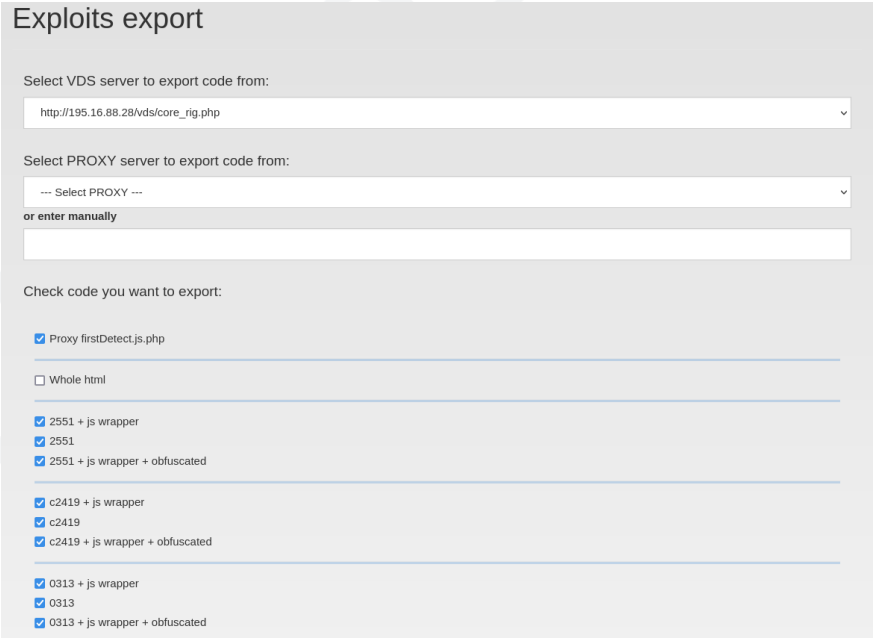

Figure 10. Exploit export page.

4.4 Malware Distribution

RIG has been used to distribute different types of malware, mainly stealers, overtime. A list illustrating the malware the PTI team has observed is portrayed in Table 1.

Filename	Hash	Classification
Alx2v5WmfMzV.exe	4c4932a64047e4aa34c3fb1bcd96521e	Gozi
anKLpKggm0gb.exe	e449924b8aa04fa2e032511cf86d2482	SmokeLoader
deATop5N2riMx0.exe	12fbb4571b89a9f14375b69c71723834	RaccoonStealer
KartOJeqhpcZL.exe	b6a06875808f59fdaaeb0eda56fe9a5b	PureCrypter
mrKT46PWXuW.exe	a48b99060695e584be29e2b816e53318	RedlineStealer
NMlsYSYm6dJK.exe	8bc77b7338da0b9041a488f185355e84	RecordBreaker
thm9KeCpkS.exe	b300ff2b8a0a2ba3130f92507e3c2b2a	RedlineStealer
vUPGMCwp.exe	c66bd22aaaae16bedd0b52ead7c32a5e	IcedID
myRFF6ZaFeo.exe	3e2332c574ae88f8fbf6a9fc9e007e65	Raccoon Stealer
YbNFQmhF.exe	7f8a2b842948eb70133fa34f0cfe772b	ZLoader
A6aTTgla.exe	6a2f114a8995dbeb91f766ac2390086e	TrueBot
6Dyn175na1.exe	def3951faab3701d653228389fc7b5fc	RaccoonStealer
DanfUz8YgFw7Ee.exe	6b6db262e0ac7c36a449692894d12ed1	Dridex
DAnFuzAaX9JE4n.exe	d43fa3957b4004ebdbe5073f99a32c9e	Dridex
mag5Wip3Ide.exe	c6cc42b429c26e68deec777eedb4c11d	Dridex
GerxIflwewM.exe	4ed2076ec15170d68a88d8b4db34fff1	UrSnif
gErVP6ZddBw.exe	6b3d119e8c22e8670deb3a4f79646495	Royal Ransomware
DVqj6UhQ.exe	6cb6a59dc12494d5c5224fc03eb12ece	Royal Ransomware

Table 1. Malware samples RIG EK was observed distributing

This is only a small glimpse into the myriad of malware that RIG EK has been observed distributing. It is also used to distribute other types of malware from various groups. A more complete list of hashes can be found in Section 8.

5 De-Anonymization

This section is intentionally redacted for the public and is only available for law enforcement officers and trusted partner companies. Feel free to ask for a copy of the private release of this report.

6 Statistics and Observations

It is interesting to point out that the exploit kit got traffic from the **207 countries**. The following chart (Figure 11) shows the exploitation attempt count per country (and dependent areas) for two months.

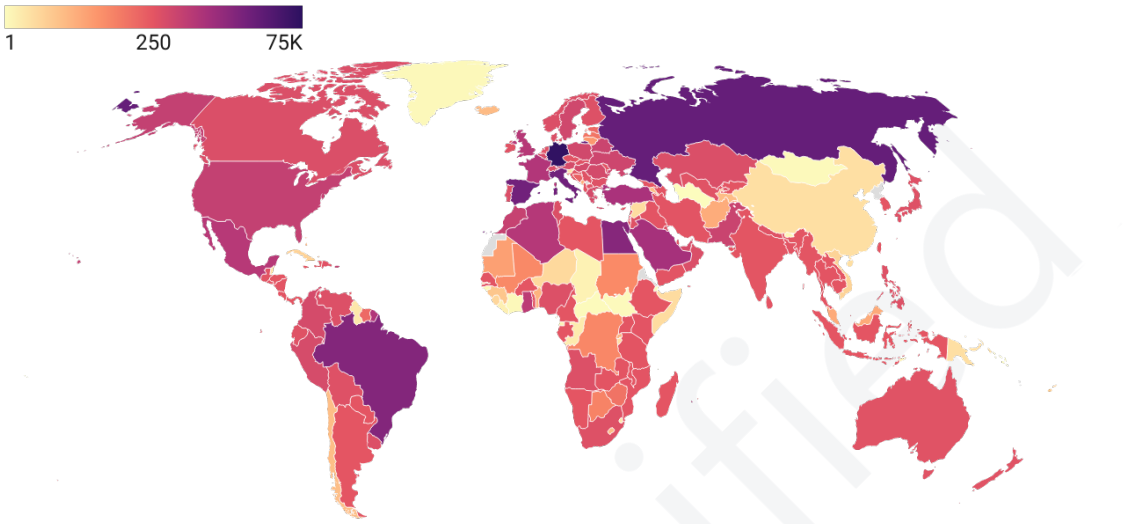

Figure 11. Exploitation attempts per country.

Exploit kit had **22%** (17647/81220) success rate in the last two months before its shutdown in 2021. The following chart (Figure 15) shows the successful exploitation attempts by country.

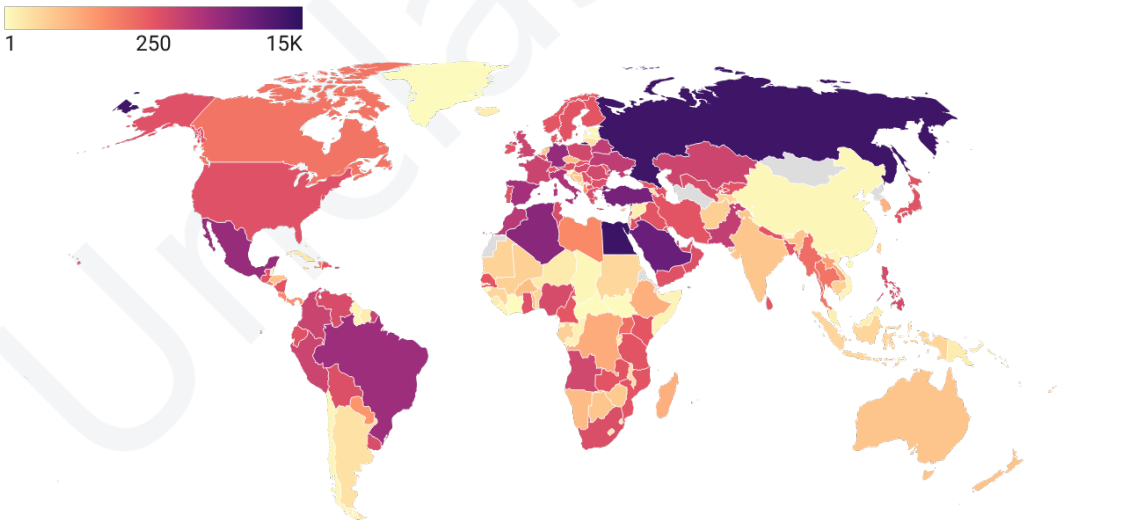

Figure 12. Successfully exploited machines per country.

Analyzing the exploitation attempt rates per day of week and percentage of successful exploitation also reveals some interesting trends. Taking a look at the chart below :

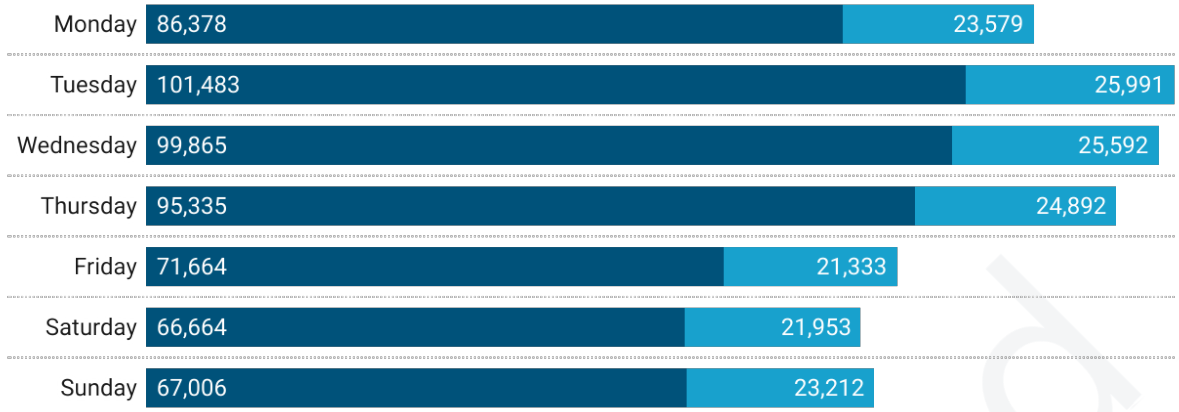

Figure 13. **Exploit attempts and successful infections per day of week.**

The RIG EK receives traffic from thousands of victims per day thanks to its malvertising campaigns. Nonetheless, what is most important for an exploit kit is the rate of successful exploitation. During its resurfacing at the end of 2022, it has consistently achieved a 30% exploitation rate among its victims. Even though throughout its lifetime, it has used numerous exploits, it has achieved the highest successful infection rate with CVE-2021-26411.

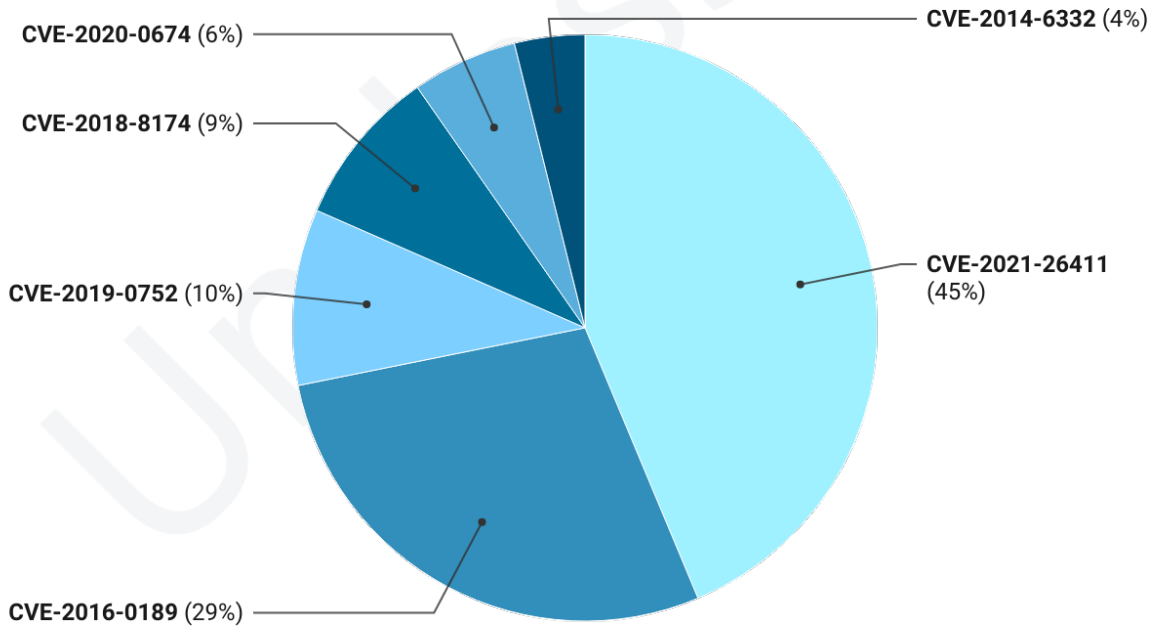

Figure 14. **Successful exploitation rate per discovery date of exploit**

As RIG EK is being distributed as a service model, it can distribute different types of malware, whilst all of them belong to different people and serve various purposes. However, statistics have showed us that most of the distributed malware are stealer examples.

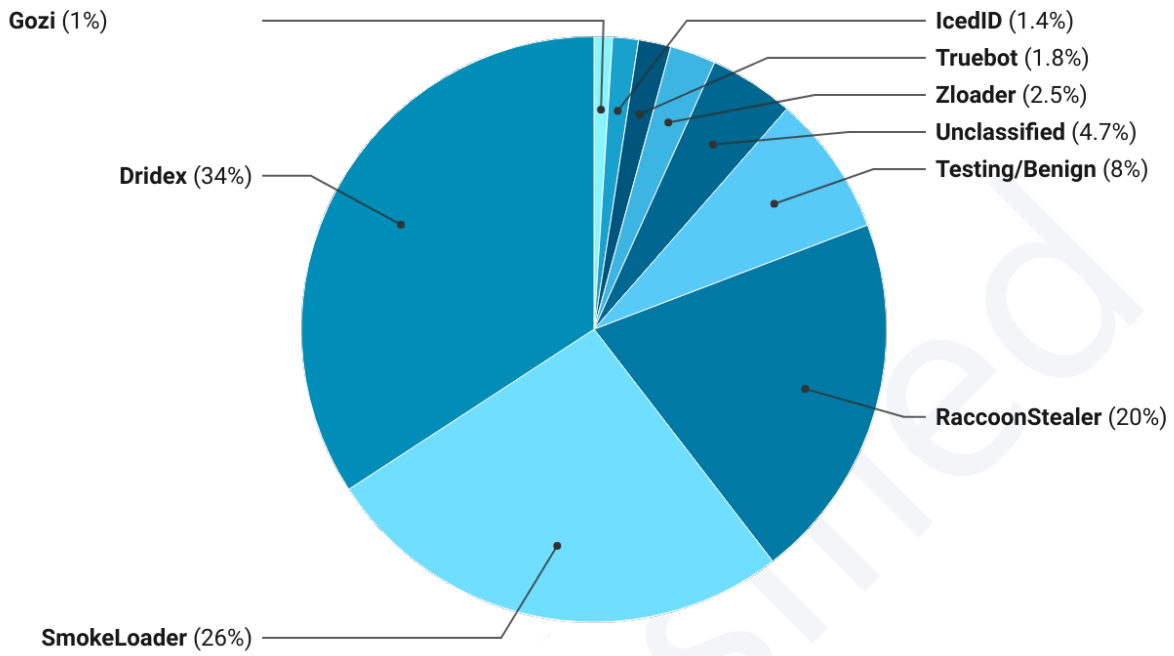

Figure 15. **Distribution percentages per type of malware.**

Overall, RIG EK runs a very fruitful business of exploit as-a-service, with victims across the globe, a highly effective exploit arsenal and numerous customers with constantly updating malware. There are only a handful of countries that has managed to stay untouched by its campaign and it receives a considerable amount of victims everyday.

7 Conclusion

This report focuses on researching and analyzing detailed information related to one of the most prominent exploit kits - the so-called **RIG EK**. As this exploit kit recently increased its activities, the report presents the reader with relevant data related to the C2 panel, new developments, threat actors in charge, technical evaluation, victim targeting and other operational details.

RIG EK has been on the scene since 2014 and due to its long-lasting activity, the type and version of the distributed malware are always changing. With **Dridex** being observed as the most common malware that is being dropped, targets are predominantly vulnerable machines that run outdated versions of Internet Explorer, making it easier to install the malware on them. The infection mainly happens through **malvertising** and **visiting compromised sites** and without any further action on the user side. Thanks to 2 new exploits, **CVE-2021-26411** and **CVE-2020-0674**, the exploitation rate reached **30%** in 2022. Financially motivated, the operators of RIG EK have the goal to gain access to victims' computers and further distribute and sell that access to other threat actors.

Furthermore, they managed to intercept victim traffic from 207 countries, with the most successful campaigns coming from Russia, Mexico, Brazil and the Middle East. Interestingly enough, the exploit try rates were the highest on **Tuesday**, **Wednesday** and **Thursday** - with successful infections taking place on the same days of the week. It is also noteworthy to mention that in addition to Dridex, the other popular types of distributed malware were stealers, such as **RaccoonStealer** or **SmokeLoader**. The report also highlights the advanced features of RIG EK, such as its use of proxy servers which makes infections harder to detect, and its integrated Antivirus testing feature, which controls for malicious software and whether any popular antivirus software caught it. The report assesses, with high confidence, that the developer of the Dridex malware has a close relationship with the RIG's admins, which further emphasizes the **sophistication and evolution** of RIG EK over the years.

In conclusion, the RIG EK exploit kit is **a significant threat** to corporations and end users. Its ability to infect devices with little to no interaction from the end user, coupled with its use of proxy servers, makes it harder to detect. The report highlights the need for organizations and individuals to remain vigilant and keep their software up-to-date to protect against this exploit kit and other similar threats.

Acknowledgement
We would like to thank our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our github page [6]. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

6. https://www.github.com/prodaft

8 IOC

8.1 Proxies

```
188.227.106.162
188.227.106.81
188.227.106.83
188.227.57.93
188.227.58.144
188.227.58.152
188.227.59.52
195.16.88.28
45.138.26.51
45.138.26.89
45.138.26.93
45.138.26.94
```

8.2 White-listed IPs

```
188.225.75.54
45.132.226.177
```

8.3 Exploit Servers

```
195.16.88.28
```

8.4 Distributed Samples

```
0773d5b2b39b964d5cdc4883e249564c697b6fee222caeed2ead3b0c7dad13c4
078ca38607f24fd21a563fa5189843734677b98d5017d5ebb03b2960053b25b5
0a59f083b2e7e919ad75c38df302283deace71ad4106fe22685e290b504e860f
11ad03c89b363353ce776edaa00cb52a71f37e6e189bce97d56859b72eca312a
148c2c5b82b22f83365e60b3494a42b1b1def3a19e086ba15a409cc2fbd50f01
1d3440fb24a7347ce312d135f138e829acc8b41f94a9491d1d195a257557f4a9
1eff4b54c1c2efc1e10fd49ef41386ab918c1c2e2c296221a85b812a7ad52e43
30f025e2a0b486f8a161eca4b4ca1df721cb1e0a6eab97ecd7e78afd0894fa6a
3c0145066c3e5b65134f6a157e26b1d6f49b2690f7aa684c70015e605a4f67f0
3c0f15094521a8677c186664573964cf9e0ab6d45c0540ee005a816465b1de51
3db1507069c0251f8a38ebac572798ecfc01856cb5febcb3f1b2fc9593b5bb1f
41a78aadb442254b6f68805375a3c7de630cd784aa739e51390da7b7ffa7fb83
49600d1fcbe50d40816e1588eacbf4b013b2951b55c9dfbf47735f1c868d72c0
4ea543e3a45ed569a9f4f4bfa7c396a0e49c360f8ed304045f7799c73d5d915a
529f5f92656efa3c8bd13c4a463b3f2550e1b4e7096426900da8de0d4fc43e44
57fc3ccdbf6ef5d5a9cc2ee339151726167b67d2678203a7174c3e3b79e9ff28
5826e055857331d129b88765c9e5a77322f4e36a336c812c502c8b87c51e503a
594a43692deac6a19744b687a29e23dc2d5f425ad17e1e0abbb556c037bdbfb5
5958a682ac3dc146b53e4bcb80f8c250ecc9ecc573e292b465de2b8daf2c8a96
5963424f5de77627224de02039d01e6693b8e267fc04f914e82c52b492e7c794
642511ccfe08d4dbcc2d7056278642d5ed9f9fb93dabeee442e28abf969691bb
69313a6cf63eafab288b2e1d23767243887568b5f10a55e128426f62938f8405
```

```
6f4d3a71ac731c8fbd21dda98b6a7a585569d9c8eaac4a1476a9f91b3f899582
72813522a065e106ac10aa96e835c47aa9f34e981db20fa46a8f36c4543bb85d
72b4b2922c575e9a801ece637bfde4154368baf17055881876ae174a5d920ae7
732eaa1e4d585156f4df6eecbbe73f6555ef0e23eca126e86686d5bc02f4be09
77c0a32673e08c2ae14b2846f678b7763785f5253b39eb45888f4a3b75297a09
7c96aeef8194d246210e843f3b9c3c6482a9a8ce5f706463fe5efdd06c81ef8d
829ec000ca31cafdf9ca32222077126d9a82dd857a4353bf2eea269cbe1edbdf
831ab9985f48fa2ad45da96b2dfba5eff98f4b18ba10c0ce12c8b3ffa687cd01
83f61982f8afe07127590669f261f08737f3cdc89b7abf8a543f3d95c2562f2f
869de7797af7c2a59e0597eaf752706acbbffde05f8c3f49c89e4a323999f460
9758f5352b7db9e60b6a935e65ad131d5de29e236133456846544dce0949fc5b
a69ee818693bfa3e1cc3999b243cf61948d238e5e7791b1d43952d961f150cd6
ac1dd32c41f6002bdf2eb564653ff23e069594ce55f9e22093355084ee28a6fd
ada01d4123accf798ba38ee21dd2dd5a813255f9a5143acb714d390ae03e967c
b070c9601e7ab97793ed65b5fc43694fb8cb1ca531240dffd0090e6cda259bde
b378914aca1901f23b5b213baae490c92a4eed43f78c7bdd25cebae92393af96
b9fd7622c3fcfdd6eb9b2cb917a3cb64eb35c61221de4866303ca88d828d5bed
bfcc9508bd3176186f186c639c797e317733eac4350e80a56cf9f417008ddae1
cb2ed19eef732c1c5f493ca7c8fc1ede57cf3bfd3e8887c522865ce0eabe449a
d5391582f00ac861712b5a810e26bb0355688c12fec74f956df28778a601b883
d83494cfb155056118365455f5396401e97bd50a156242f2b5025a44c67095b1
ed11dc8f2282bd070f44afcb725202f42a77d807c69219f18a6b3460a3c8e68f
f19f501beaf1cf4d8a2d0f0495d20749ec2086f1b52205779060028ffe6a81f9
```

Références

[1] Malware Traffic Analysis. *RIG EK Sends Ramnit, Follow-Up Malware : Azorult*. url : https://www.malware-traffic-analysis.net/2018/01/30/index.html. (accessed : 07.04.2022).

[2] BleepingComputer. *RIG Exploit Kit Suffers Major Blow Following Coordinated Takedown Action*. url : https://www.bleepingcomputer.com/news/security/rig-exploit-kit-suffers-major-blow-following-coordinated-takedown-action/. (accessed : 17.12.2022).

[3] New Jersey Cybersecurity & Communications Integration Cell. *RIG Threat Profile*. url : https://www.cyber.nj.gov/threat-center/threat-profiles/exploit-kit-variants/rig. (accessed : 07.04.2022).

[4] DarkReading. *RIG Exploit Kit Replaces Raccoon Stealer Trojan With Dridex*. url : https://www.darkreading.com/attacks-breaches/rig-exploit-kit-replaces-raccoon-stealer-trojan-with-dridex. (accessed : 15.12.2022).

[5] ESET. *Read The Manual : A Guide to the RTM Banking Trojan*. url : https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf. (accessed : 27.12.2021).

[6] Malwarebytes Threat Intelligence. *RIGEK dropping RaccoonStealer*. url : https://twitter.com/MBThreatIntel/status/1479155809703522306. (accessed : 07.04.2022).

[7] Palo Alto Networks. *CryptoBit : Another Ransomware Family Gets an Update*. url : https://unit42.paloaltonetworks.com/unit42-cryptobit-another-ransomware-family-gets-an-update/. (accessed : 07.04.2022).

[8] TrustWave. *RIG Exploit Kit – Diving Deeper into the Infrastructure*. url : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rig-exploit-kit-diving-deeper-into-the-infrastructure/. (accessed : 07.04.2022).

Historique

Version	Date	Auteur(s)	Modifications
1.0	19.10.2021	PTI Team	Initial TLP:RED DRAFT release
1.1	25.10.2021	PTI Team	Updated De-anonymization section for LE
2.0	23.01.2023	PTI Team	TLP:RED Version
3.0	27.02.2023	PTI Team	TLP:CLEAR Version