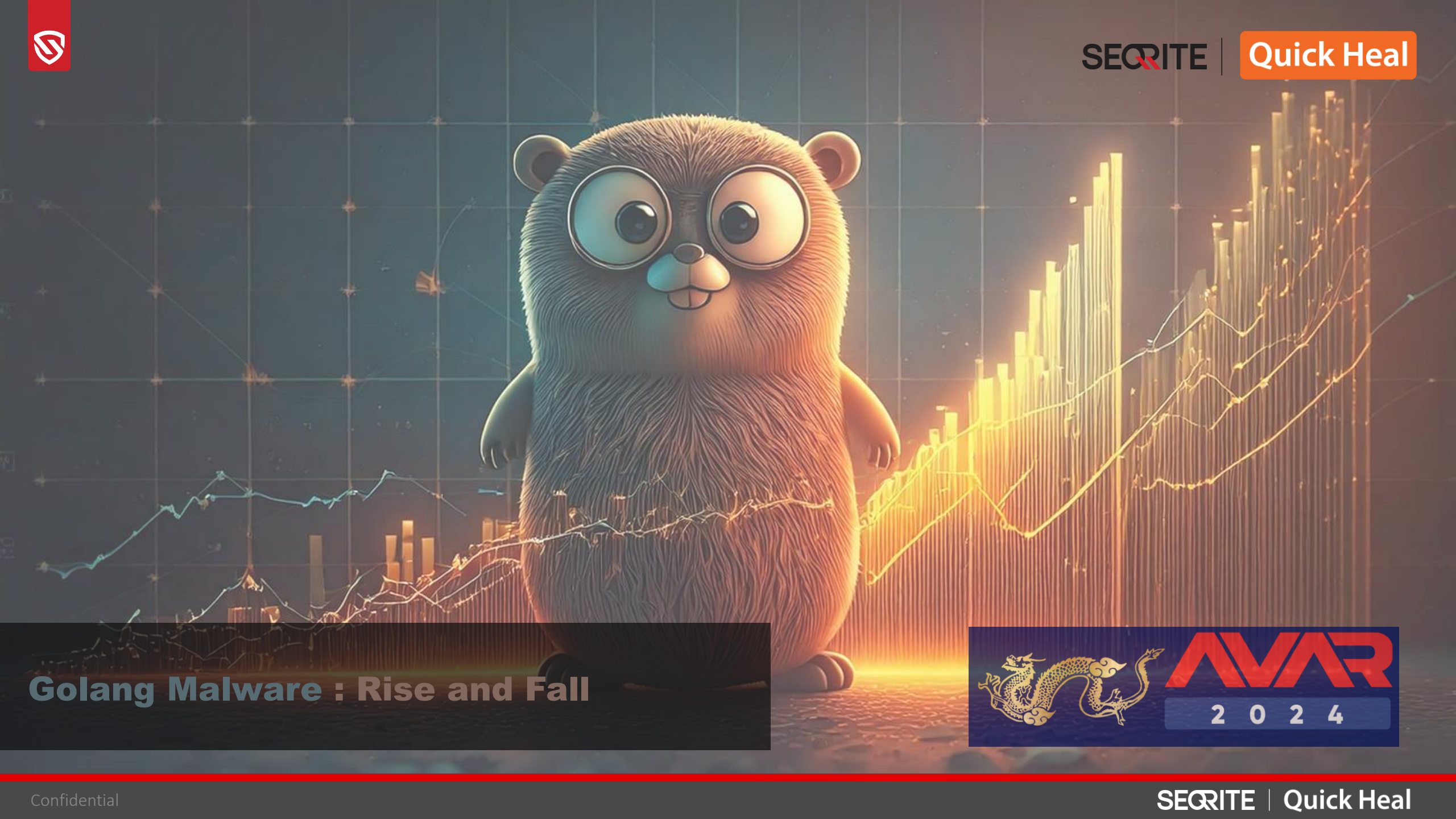

SECRITE | Quick Heal
Golang Malware : Rise and Fall
AVAR
2024

$whoami

- **What I do ?** Threat [Detection | Hunting | Intelligence]
- **Where ?** Seqrite Labs , Quick Heal , India

@ElementalX2

Subhajeet Singha

Agenda

01 Contents.

02 Rise of Trend.

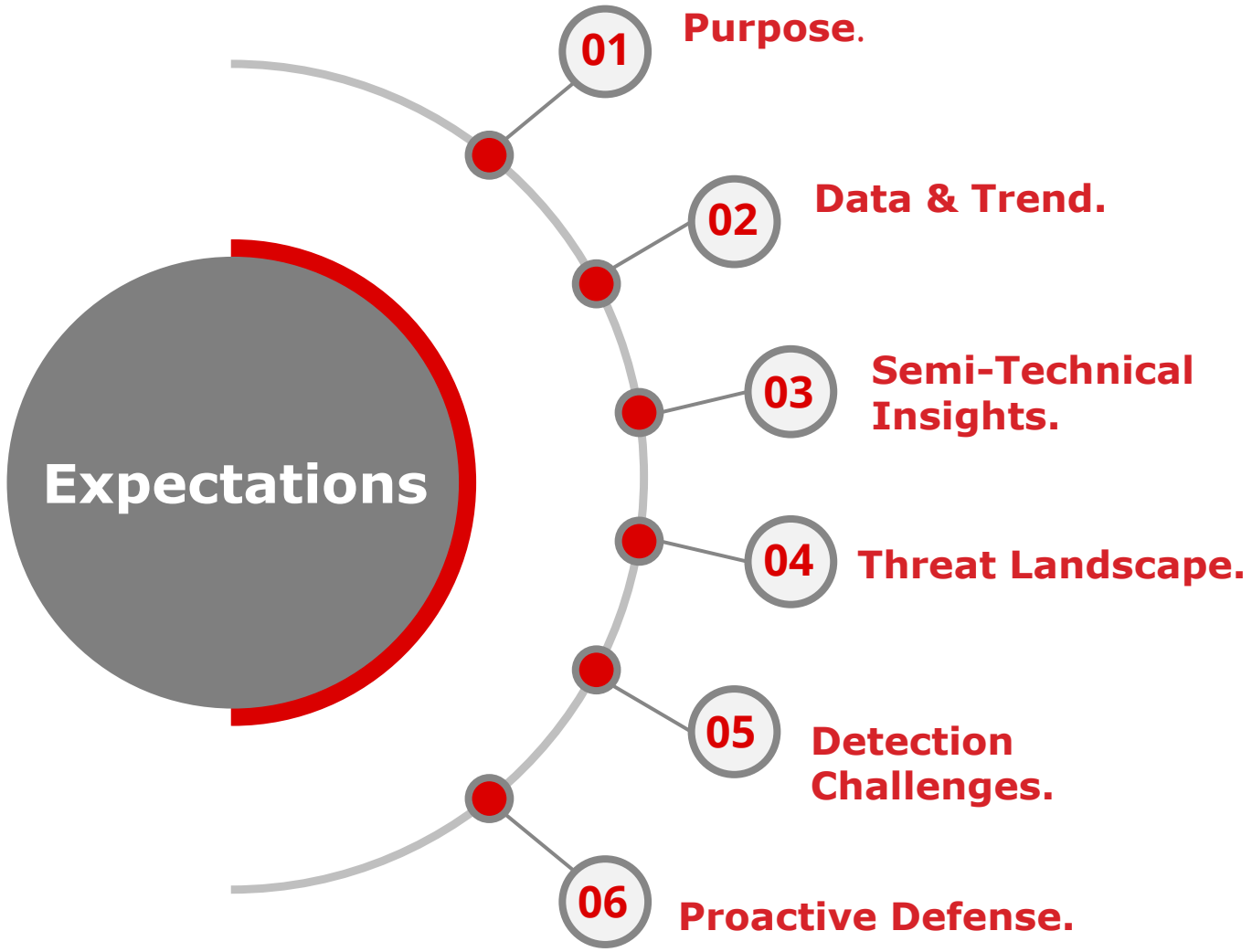
03 Fall of Trend.

04 Pseudo-Rise.

05 Tool Demo : Go-Peep.

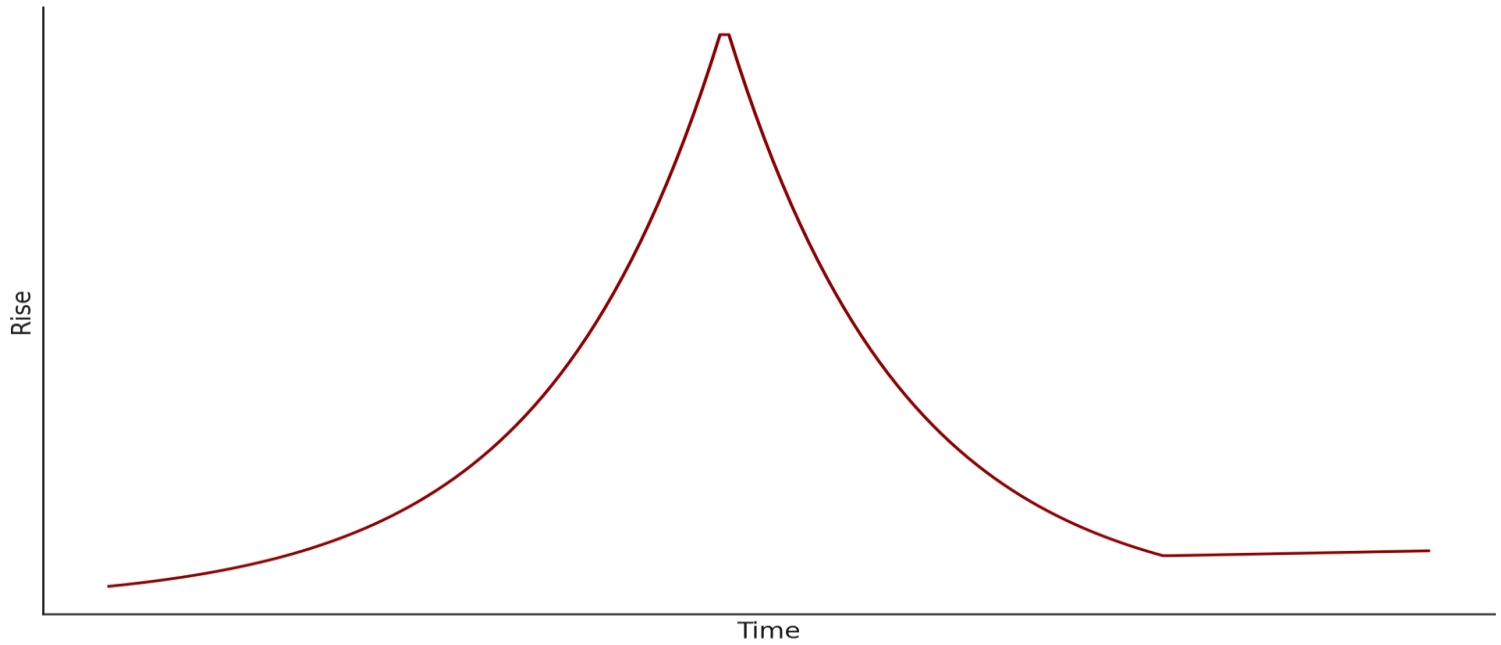
CONTENTS

CONTENTS


Expectations
01
Purpose.
02
Data & Trend.
03
Semi-Technical Insights.
04
Threat Landscape.
05
Detection Challenges.
06
Proactive Defense.

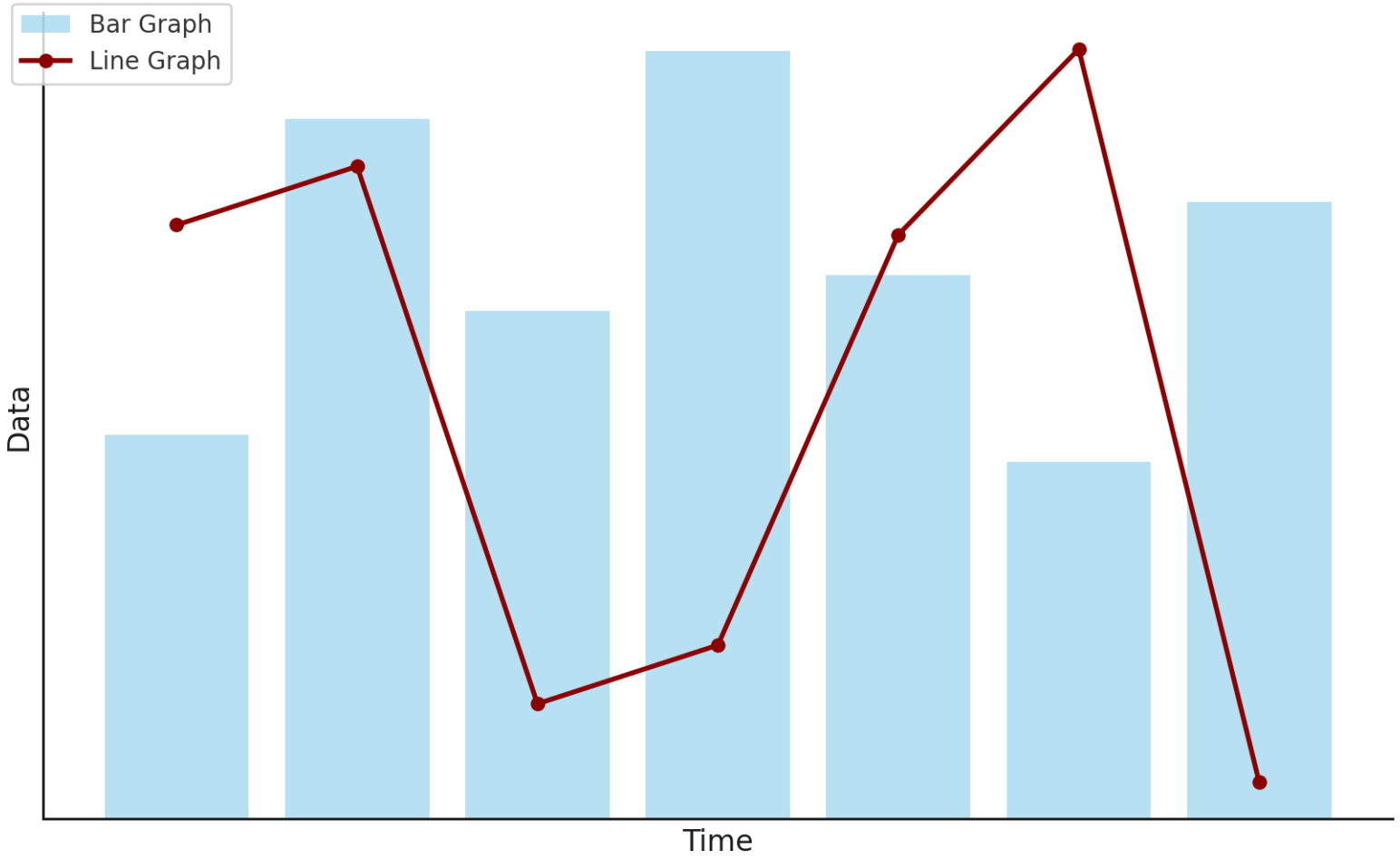
CONTENTS

01 **Purpose :** Highlight the goal of understanding Golang-based malware trends and its implications for malware defense.



02 Data & Trend

Provide statistical data showing the rise of Golang malware and geographic distribution trends.



CONTENTS

03 Semi-technical Insights

Offer insights into the semi-technical aspects of Golang malware, including code characteristics, libraries, and structures that have influenced its rise.

04 Threat Landscape

Explore the impact of Golang malware on global cybersecurity, specifically addressing notable campaigns (state-sponsored and ransomware) and widespread infections

05 Detection Challenges

Explore how the anti-malware community and other vendors have faced a lot of challenges and how they did overcome from this.

CONTENTS

06 Proactive Defense

Detail advancements in early detection techniques, specifically focusing on open-source repositories and tools like Go-Obfuscator, Garble that are aiding Golang malware developers giving a pseudo-rise.

CASE STUDY : RISE OF TREND

CASE STUDY : RISE OF TREND

CLAIMS FOR "RISE OF GOLANG MALWARE"

- Increased Prevalence of Golang Malware.
- Diverse Use Cases of Golang in Cyber Threats.
- Geographical Spread of Golang Malware[APT].
- Impact of Golang in High-Profile Threat Campaigns.
- Accessibility and Flexibility Fueling Malware Development.

Time to debunk ?

CASE STUDY : RISE OF TREND

Claim: Increased Prevalence of Golang Malware.

"In the past five years, there has been a significant rise in Golang-based malware In-The-Wild (ITW), indicating a growing trend in its adoption by threat actors.''

CASE STUDY : RISE OF TREND

SECRITE | Quick Heal

Malware Uses Google Go Language

Sep 18, 2012 05:50 PM

Migration User

Designed in 2007 and introduced in late 2009, the Go programming language developed by Google has been gaining momentum the past three years. It is now being used to develop malware. Recently seen in the wild, Trojan.Encriyoko is a new threat associated with components which are written in Go. The Trojan attempts to encrypt various file formats on compromised computers, rendering the encrypted files unusable.

The original sample we acquired, a file named GalaxyNxRoot.exe, is actually a dropper written in .NET which disguises itself as a rooting tool to trick users into installing it.

Where it all started?

Andrew said it before it was cool!

CASE STUDY : RISE OF TREND

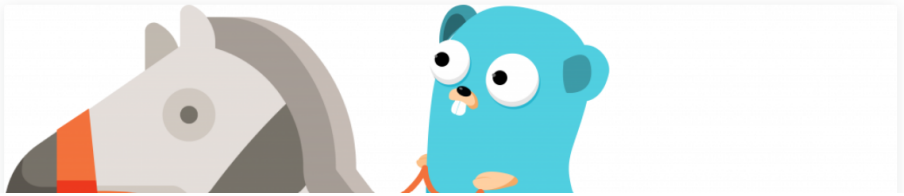
SECRITE | Quick Heal

Sofacy Creates New 'Go' Variant of Zebrocy Tool

39,969 people reacted | 5 | 10 min. read

SHARE

By Robert Falcone
December 18, 2018 at 6:00 AM
Category: Unit 42
Tags: Sofacy, Zebrocy



2018 – 2019

Early Notable Trends

National Cyber Security Centre
a part of GCHQ

Advisory: APT29 targets COVID-19 vaccine development

// AUTHORS

IVAN KWIATKOWSKI Expert FÉLIX AIME PIERRE DELCHER

On December 4, 2019, we discovered watering hole websites that were compromised to selectively trigger a drive-by download attack with fake Adobe Flash update warnings. This campaign has been active since at least May 2019, and targets an Asian religious and ethnic group.

The threat actor's unsophisticated but creative toolset has been evolving a lot since the inception date, may still be in development, and leverages Sojson obfuscation, NSIS installer, Python, open-source code, GitHub distribution, Go language, as well as Google Drive-based C2 channels.

The threat actor's operational target is not clear because, unfortunately, we haven't been able to observe many live operations, and we couldn't identify any overlap with known intrusion sets.

NEWS | THREATS

Analyzing a new stealer written in Golang

Posted: January 30, 2019 by hasherezade

Golang (Go) is a relatively new programming language, and it is not common to find malware written in it. However, new variants written in Go are slowly emerging, presenting a challenge to malware analysts. Applications written in this language are bulky and look much different under

CASE STUDY : RISE OF TREND

There's a New a Golang-written RAT in Town

Silvia PRIPOAE
October 09, 2020

CRIMEWARE

New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware

JIM WALTER / JANUARY 23, 2020

We are just about 1 month into 2020, and so far, there has been no break in the ongoing flurry of new or varied ransomware campaigns. Amongst the well-established families (Ryuk, Maze, REvil) we now have another to add to the list..."Snake".

SentinelLabs has observed the Snake ransomware in targeted campaigns over the last month. While it contains all the hallmarks of standard ransomware,

2020

Spotted between August to September 2020, **SUNSHUTTLE** is a Golang-based malware that acts as a command-and-control backdoor, establishing a secure connection with an attacker-controlled server to receive commands to download and execute files, upload files from the system to the server, and execute operating system commands on the compromised machine.

NEW GOLANG-BASED CRYPTO WORM INFECTS WINDOWS AND LINUX SERVERS

Pierluigi Paganini December 31, 2020

```
Package hello/src/exp: /media/psf/AllFiles/Users/mac/go/src/hello/src/exp
File: <autogenerated>
        init Lines: 1 to 40 (39)
File: exp.go
        NewAttack Lines: 22 to 115 (93)
        registerExp Lines: 115 to 119 (4)
        (*Attack)All Lines: 119 to 129 (10)
        (*Attack)Loop Lines: 129 to 131 (2)
        (*Attack).Loopfunc1 Lines: 137 to 138 (1)
File: jenkins.go
        Jenkins Lines: 14 to 53 (39)
        checkJenkins Lines: 53 to 61 (8)
        init0 Lines: 61 to 66 (5)
File: mysql.go
        Mysql Lines: 15 to 90 (75)
        mysql_max_allowed_packet Lines: 90 to 114 (24)
        sqlExec Lines: 114 to 130 (16)
        init1 Lines: 130 to 139 (9)
```

CASE STUDY : RISE OF TREND

Abcbot — A New Evolving Wormable Botnet Malware Targeting Linux

Nov 12, 2021 Ravie Lakshmanan

ANTI-MALWARE RESEARCH • 1 min read •

Debugging MosaicLoader, One Step at a Time

Janos Gergo SZELES
July 20, 2021

DECAF Ransomware: A New Golang Threat Makes Its Appearance

Posted by **Hido Cohen & Michael Dereviashkin** on October 28, 2021

2021

LevelBlue Labs finds new Golang malware (BotenaGo) targeting millions of routers and IoT devices with more than 30 exploits

November 11, 2021 | Ofer Caspi

TA505 adds GoLang crypter for delivering miners and ServHelper

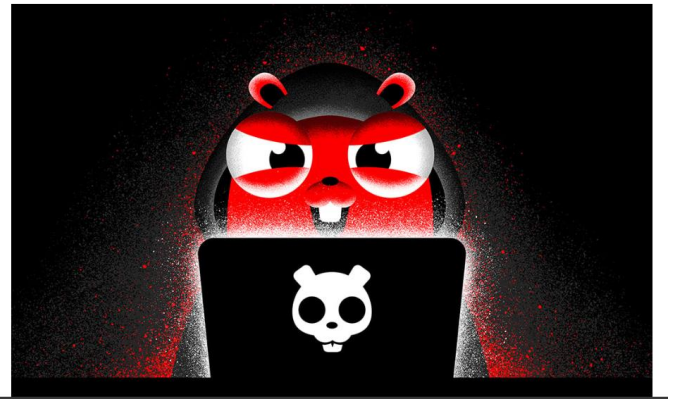
Jason Reaves · Follow
Published in Walmart Global Tech Blog · 6 min read · Jul 6, 2021

CASE STUDY : RISE OF TREND

2022

TellYouThePass Ransomware Analysis Reveals a Modern Reinterpretation Using Golang

January 11, 2022 | Anmol Maurya | Endpoint Security & XDR



HOME > CYBERSECURITY NEWS

Agenda, a New Golang Ransomware, Is on the Loose

The Ransomware Can Be Customized for Every Victim.

Last updated on October 20, 2022

Arid Gopher - A New Golang Malware Spotted in the Town

Malware and Vulnerabilities • March 24, 2022 • Cyware Alerts - Hacker News

BLOG

SECURONIX THREAT LABS SECURITY ADVISORY: NEW GOLANG ATTACK CAMPAIGN GO#WEBBFUSCATOR LEVERAGES OFFICE MACROS AND JAMES WEBB IMAGES TO INFECT SYSTEMS

THREAT RESEARCH

CRIMEWARE

CrateDepression | Rust Supply-Chain Attack Infects Cloud CI Pipelines with Go Malware

JUAN ANDRÉS GUERRERO-SAADE / MAY 19, 2022

By Juan Andrés Guerrero-Saade & Phil Stokes

CASE STUDY : RISE OF TREND

ADVERSARY

DragonSpark | Attacks Evade Detection with SparkRAT and Golang Source Code Interpretation

ALEKSANDAR MILENKOSKI / JANUARY 24, 2023

By Aleksandar Milenkoski, Joey Chen, and Amitai Ben Shushan Ehrlich

Skuld: The Infostealer that Speaks Golang

By Ernesto Fernández Provecho · June 13, 2023

In May 2023, the Trellix Advanced Research Center discovered a new Golang stealer, known as Skuld, that compromised systems worldwide, something that security researchers had also noticed.

The usage of Golang, also known as Go, in malware development is still rare compared to other programming languages. But it has gained significant popularity in recent years due to simplicity, efficiency, and cross-platform compatibility, which lets malware creators target a wide range of operating systems, broadening their potential victim pool. Additionally, Golang's compiled nature lets malware authors produce binary executables that are more challenging to analyze and reverse engineer. This makes it harder for security researchers and traditional anti-malware solutions to detect and mitigate these threats effectively.

This new malware strain tries to steal sensitive information from its victims. To accomplish this task, it searches for data stored in applications such as Discord and web browsers; information from the system and files stored in the victim's folders. Some samples even include a module to steal cryptocurrency assets, which we believe is still in development.

Detailed Analysis of AlphaSeed, a new version of Kimsuky's AppleSeed written in Golang

S2W · Follow
Published in S2W BLOG · 19 min read · May 17, 2023

Author: BLKSMTH | S2W TALON

Last Modified: May 17, 2023

This new malware targets Discord and browser data using one major unique feature

News By Craig Hale published 15 June 2023

Use of Go programming language is especially worrying, experts warn

2023

Titan Stealer: A New Golang-Based Information Stealer Malware Emerges

Jan 30, 2023 Ravie Lakshmanan Threat Detection / Malware

CASE STUDY : RISE OF TREND

SEQRITE | Quick Heal

BLOG

Operation FlightNight: Indian Government Entities and Energy Sector Targeted by Cyber Espionage Campaign

Arda Büyükkaya – March 27, 2024

2024

APT group GoldenJackal deploys backdoors to air-gapped systems

News
09 Oct 2024 • 7 mins

Kimsuky disguised as a Korean company signed with a valid certificate to distribute Troll Stealer (English ver.)

S2W · Follow
Published in S2W BLOG · 14 min read · Feb 7, 2024

Analysis of APT-C-00 (OceanLotus) Double Loader and Related VMP Loader

NetmanageIT OpenCTI - opencti.netmanageit.com

Daniel Bender
Sep 24, 2024 • 1 min read

CASE STUDY : RISE OF TREND

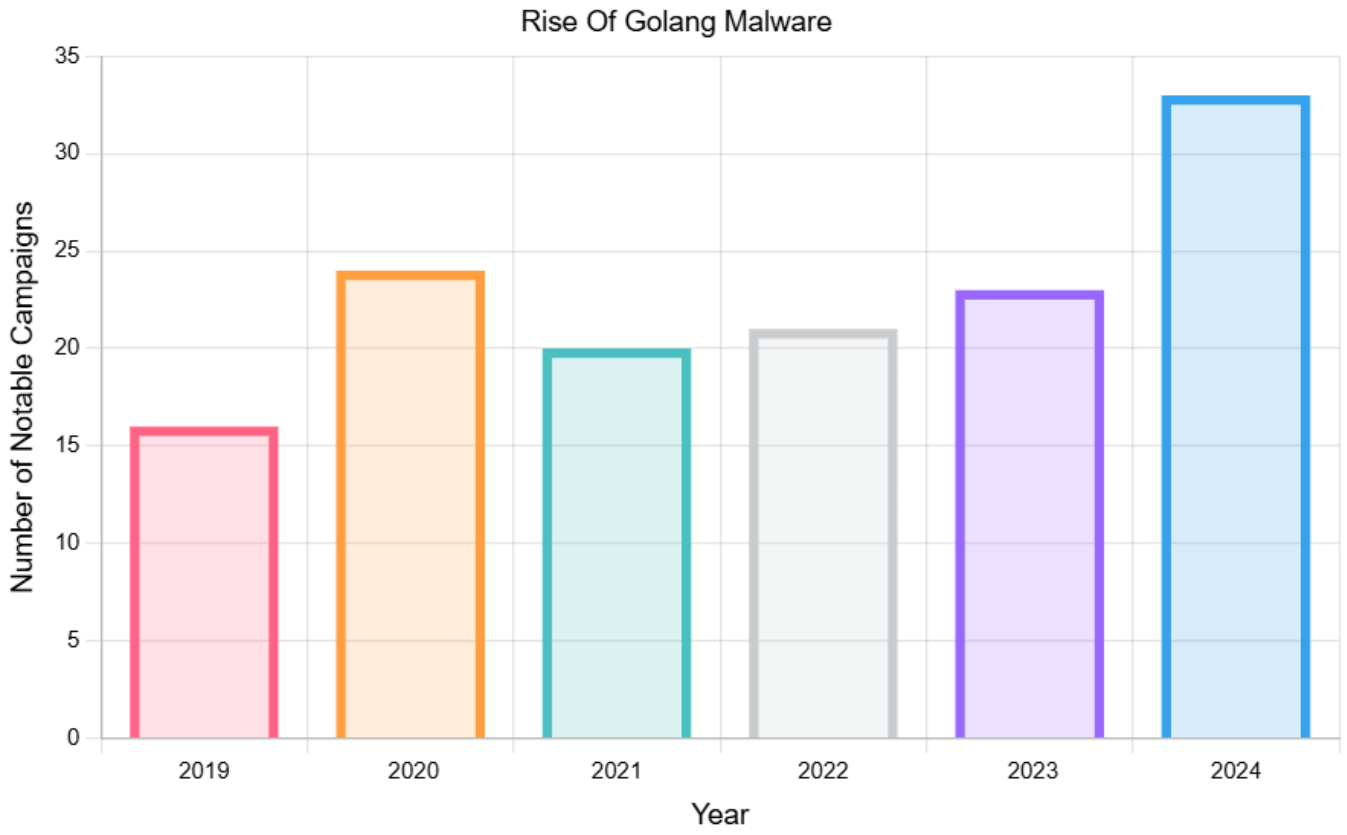
Claim: Diverse Use Cases of Golang in Cyber Threats.

"In the past five years, Golang has powered malware across ransomware, APTs, stealers, and RATs."

CASE STUDY : RISE OF TREND

- This graph has been plotted solely on the based on some interesting and notable reports of various vendors and from sources like AlienVault OTX & Malpedia only which includes campaigns related to :

1. Advanced Persistent Threat Groups.
2. Stealers / RATs.
3. Botnets.
4. Ransomware
5. Miners.
6. Wipers.



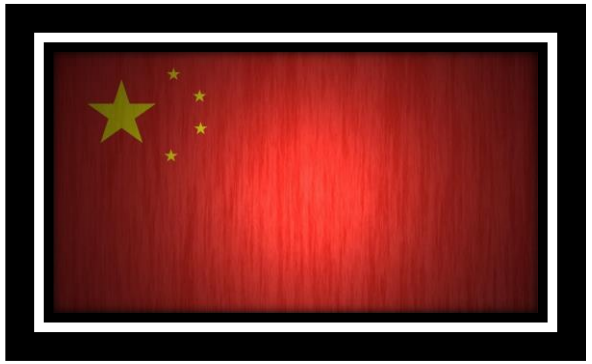
CASE STUDY : RISE OF TREND

Claim: Geographical Spread of Golang Malware[APT].

"In the past five years, Golang has been welcomed by Advanced Persistent Threat Groups across the globe”

CASE STUDY : RISE OF TREND

- APT28.
- APT29.



- TA416
- Evasive Panda
- Earth Lusca

- Kimsuky. [1] [2]
- Lazarus.

CASE STUDY : RISE OF TREND

- MuddyWater.
- APT34.

- Patchwork.

- APT-36

- Arid Viper

CASE STUDY : RISE OF TREND

Claim: Impact of Golang in High-Profile Threat Campaigns.

"In the past five years, there has been some ongoing tension across the globe, we will see how Golang has been leveraged by threat groups or actors to further execute their campaigns."

CASE STUDY : RISE OF TREND

SolarWinds Incident

GoldMax (aka SUNSHUTTLE), which was discovered by Microsoft and FireEye (now Mandiant) in March 2021, is a Golang-based malware that acts as a command-and-control backdoor, establishing a secure connection with a remote server to execute arbitrary commands on the compromised machine.

RU-UA Geopolitical Tensions.

HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine

JUAN ANDRÉS GUERRERO-SAADE / FEBRUARY 23, 2022

This post was updated Feb 28th 2022 to include new IOCs and the PartyTicket 'decoy ransomware'.

IND-PK Geopolitical Tensions.

Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages

RESEARCH & INTELLIGENCE / 05.22.24 / The BlackBerry Research and Intelligence Team

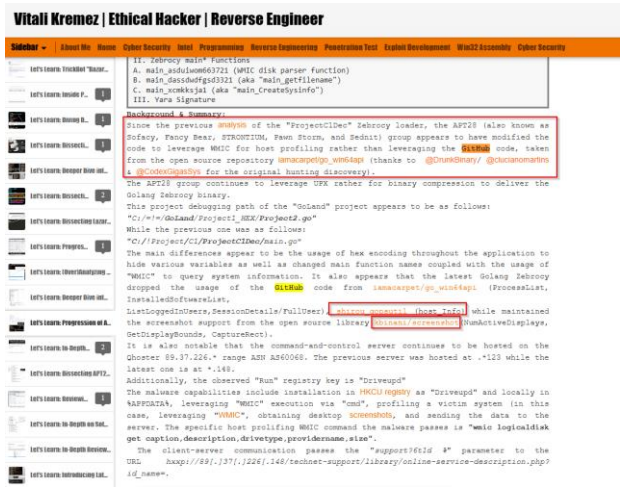
CASE STUDY : RISE OF TREND

Claim: Accessibility and Flexibility Fueling Malware Development.

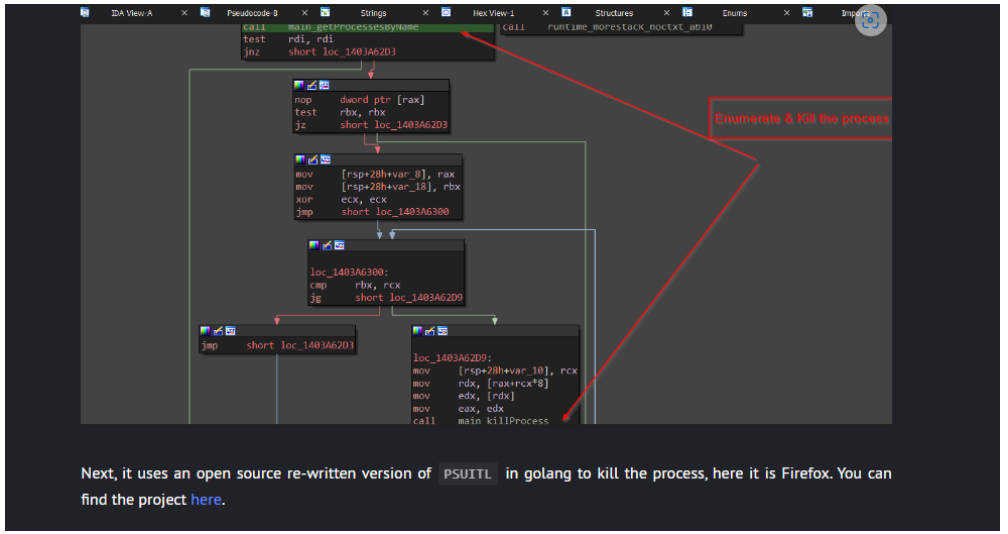
"In the past five years, Golang malware development has been accessible in means of Open-Source Software development projects and Command and Control software, with its flexibility fueling widespread adoption."

CASE STUDY : RISE OF TREND

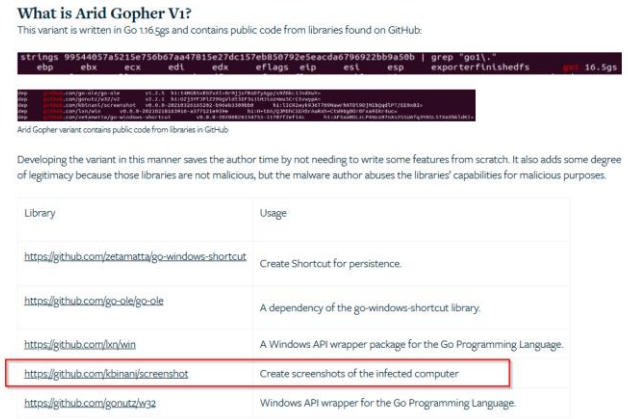
- Software Development Projects (gopsutil , screenshot)



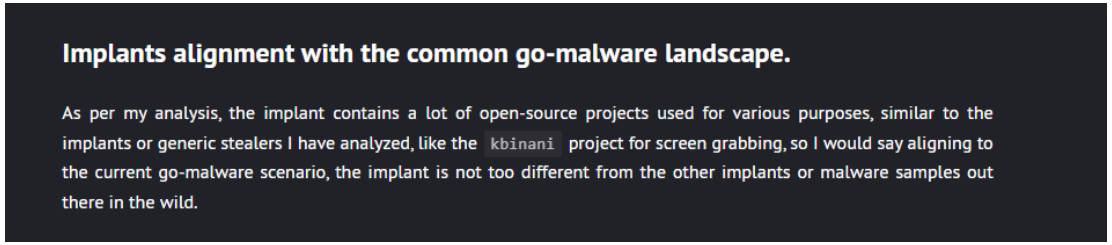
2018 : APT 28



2024 : APT 36



2022 : Arid Viper

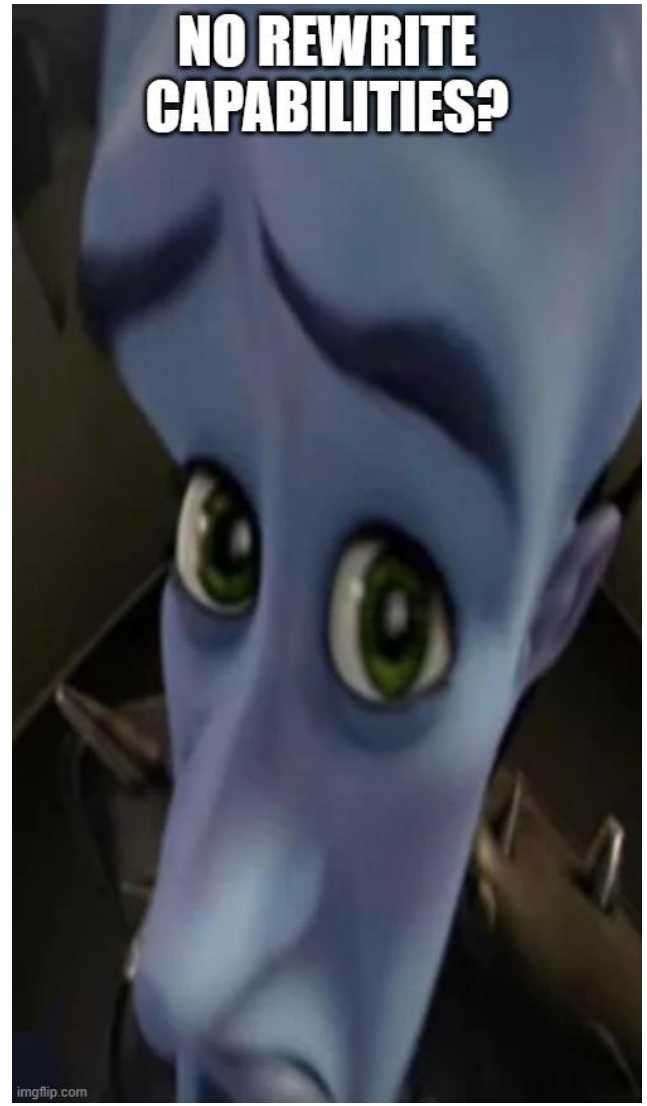


2024 : Patchwork

CASE STUDY : RISE OF TREND

Some common used projects and libraries:

- go-ole.
- os-exec.
- syscall.
- clipboard.
- crypto
- go-ps.
- debug/pe.
- debug/elf.



CASE STUDY : RISE OF TREND

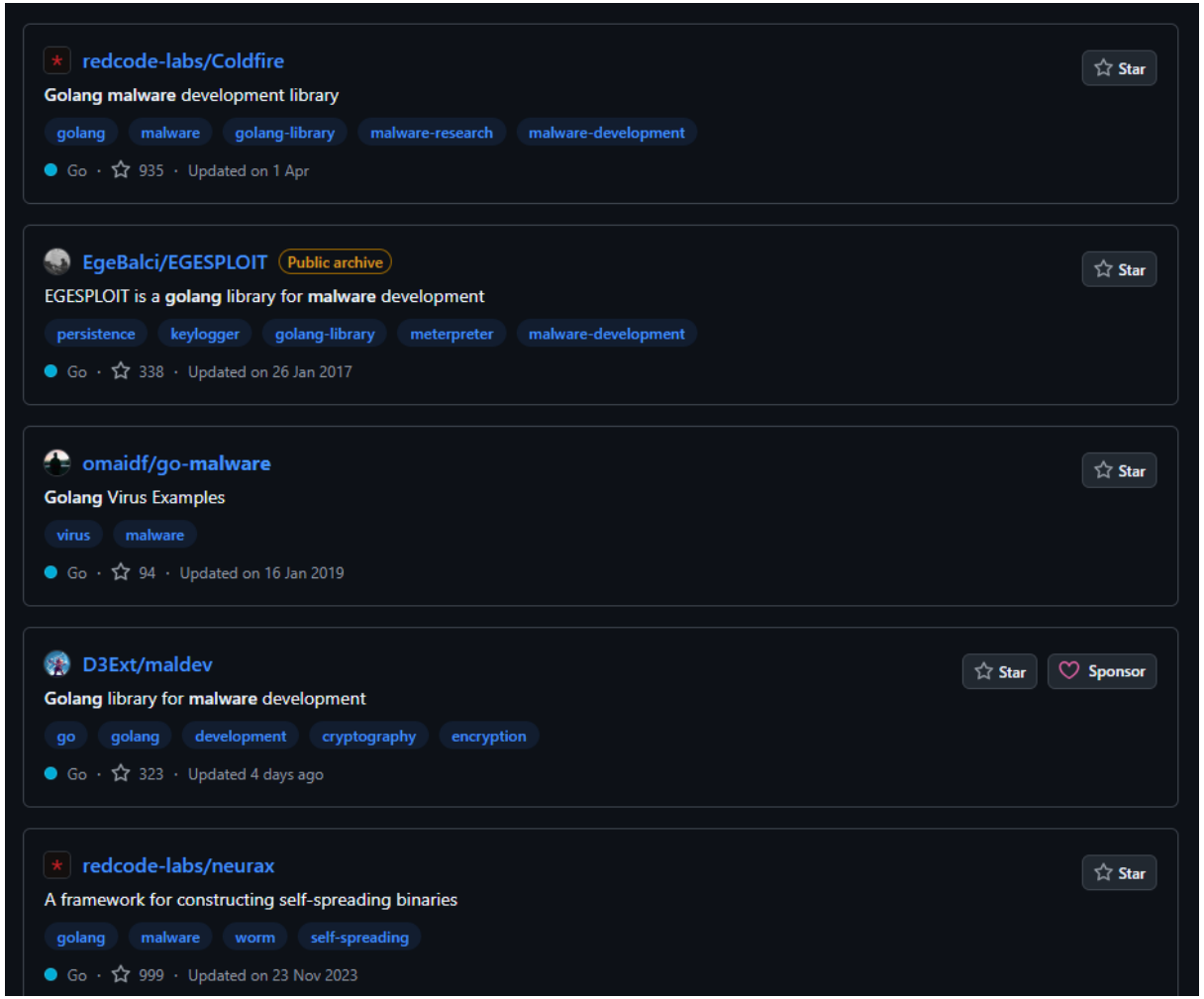
Developments in last 5 years ?

- Too many Open-Source Golang Malware projects in GitHub.
- Open-Source Command and Control Frameworks projects being used in campaigns.
- Craze among malicious software developers.
- Easily tweakable.

CASE STUDY : RISE OF TREND

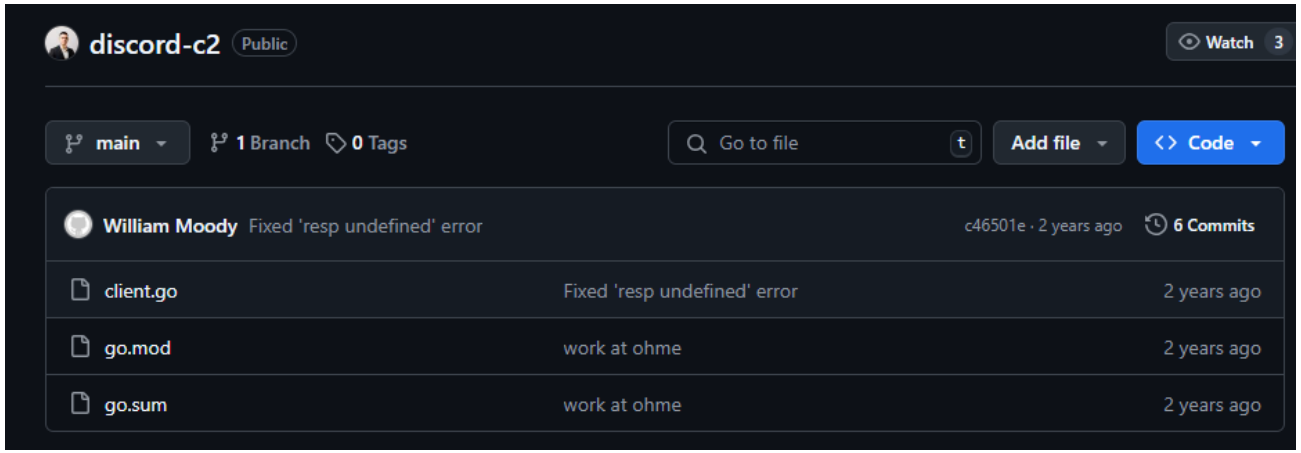
Golang Ransomware:

- target111/go-crypt - Golang ransomware
- lucasduete/ransomware-go - Ransomware implementation in Go
- kvasirlabs/pirategopher: Ransomware written in Go w/ a variety of payload options and a easy-to-deploy C2 server (github.com)
- The-Mario/Mario-Ransamware: Ransomware (github.com)
- Soldie/ransomware (github.com)
- 0xh4di/ransomware (github.com)
- andyjsmith/Bad-Gopher: POC ransomware in Golang (github.com)
- qureshijey1/ransomware-project (github.com)
- mauri870/ransomware: A POC Windows crypto-ransomware (Academic). Now Ransom:Win32/MauriCrypt.MK!MTB (github.com)
- wille/cry: Cross platform PoC ransomware written in Go (github.com)
- ejserna/Ransomware: Crypto Ransomware made with: - Go for encryption and decryption - PHP/MySQL for saving and retrieving keys. (github.com)
- gustavohenrique/ransomware: A ransomware implementation just for educational purpose (github.com)
- TheCreeper/UselessLocker: Randomware-like sample that can be easily modified and used. For educational purposes. (github.com)

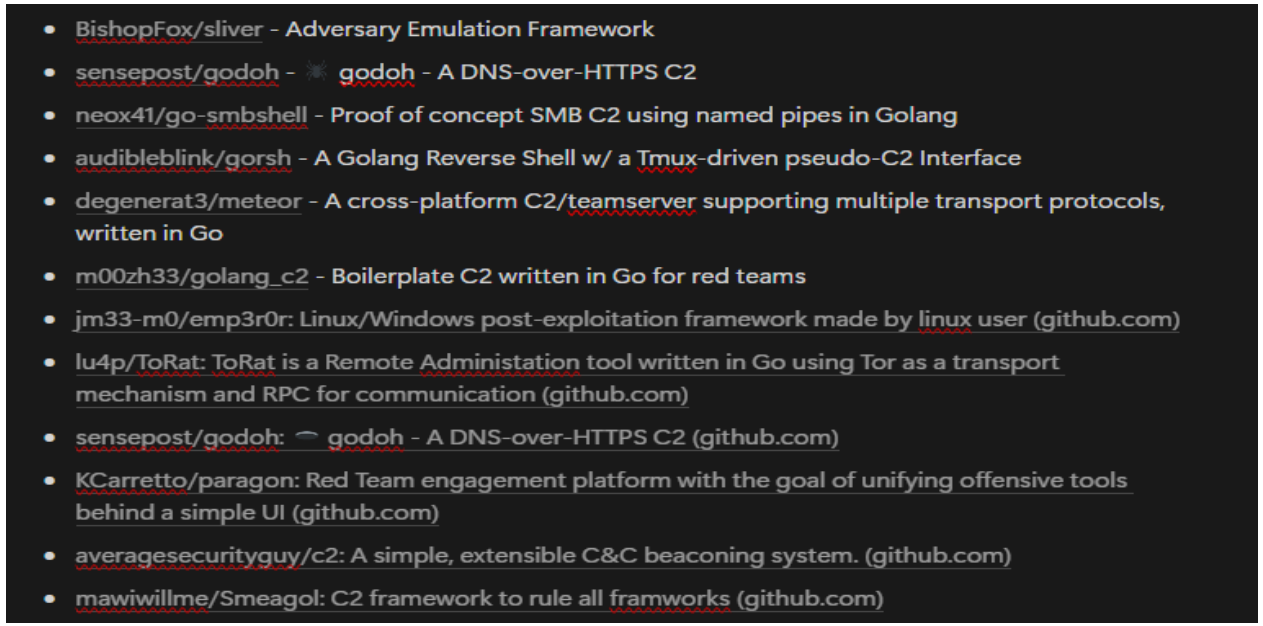


Too many open-source Golang malware projects.

CASE STUDY : RISE OF TREND

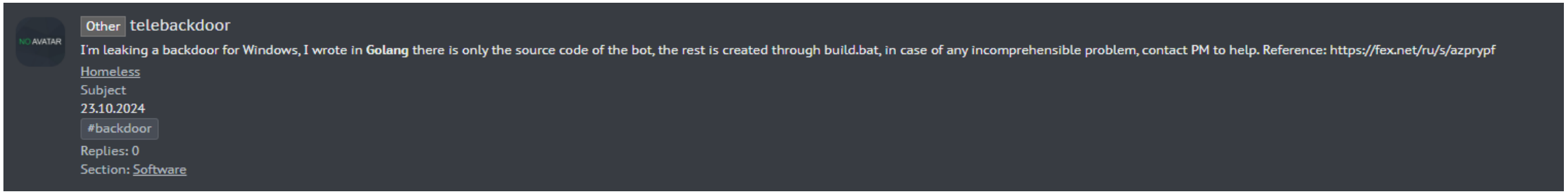


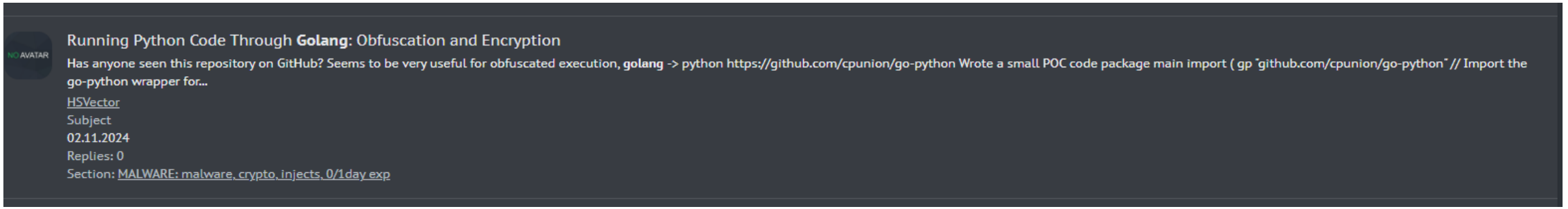
Used by Transparent Tribe / APT 36



Used by many APT groups and ransomware groups.

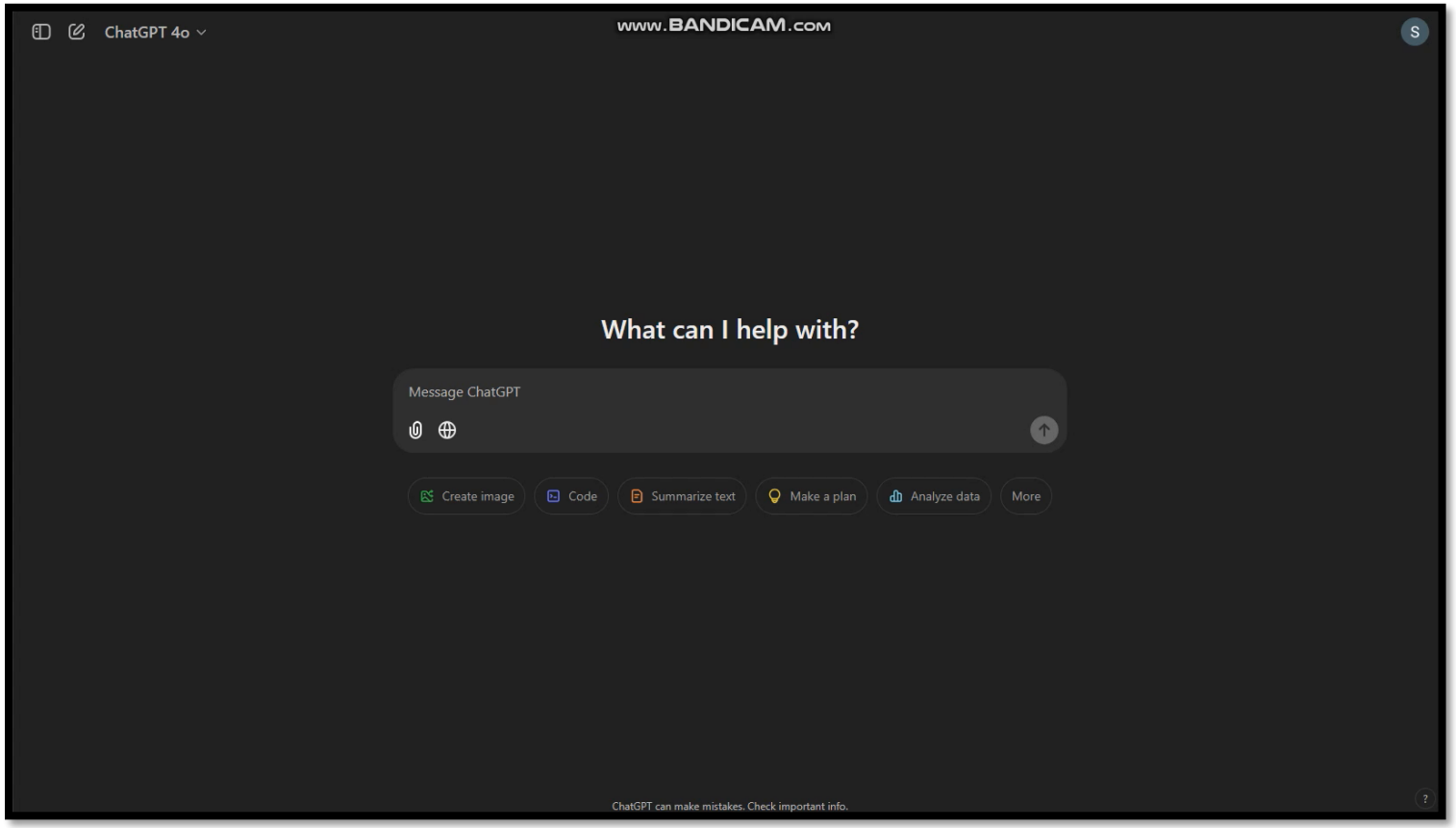
CASE STUDY : RISE OF TREND





Rise in Golang oriented topics in XSS Forum.

CASE STUDY : RISE OF TREND



Easily Tweakable & easy to write

[Even anyone with an access to GPT could do it]

CASE STUDY : FALL OF TREND

CASE STUDY : FALL OF TREND

CLAIMS FOR "FALL OF GOLANG MALWARE"

- Adaptation of Malware Research Tools and Strategies.
- Operator Errors Facilitating Proactive Defense.

    1. Unique Indicators and Artifacts.

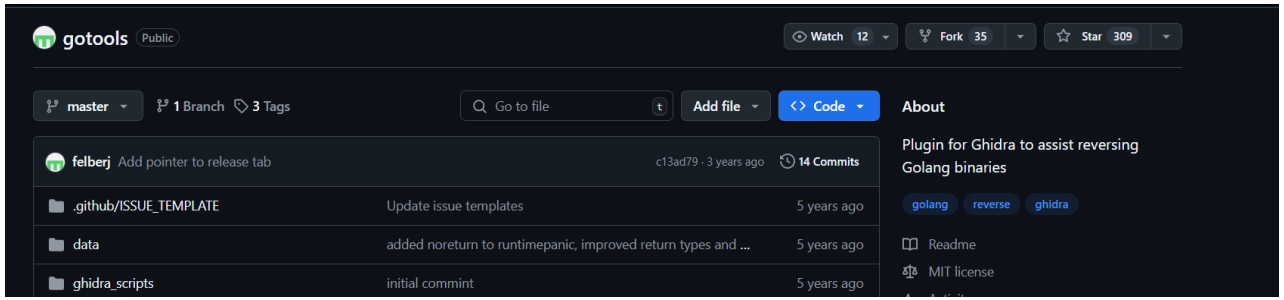
    2. Abuse of Open-Source Repositories.

CASE STUDY : FALL OF TREND

Claim: Adaptation of Malware Research Tools and Strategies.

“The rise of Golang malware prompted the development of specialized tools and techniques, including reverse engineering plugins and detection rules tailored to Golang binaries, which have significantly improved detection rates.”

CASE STUDY : FALL OF TREND

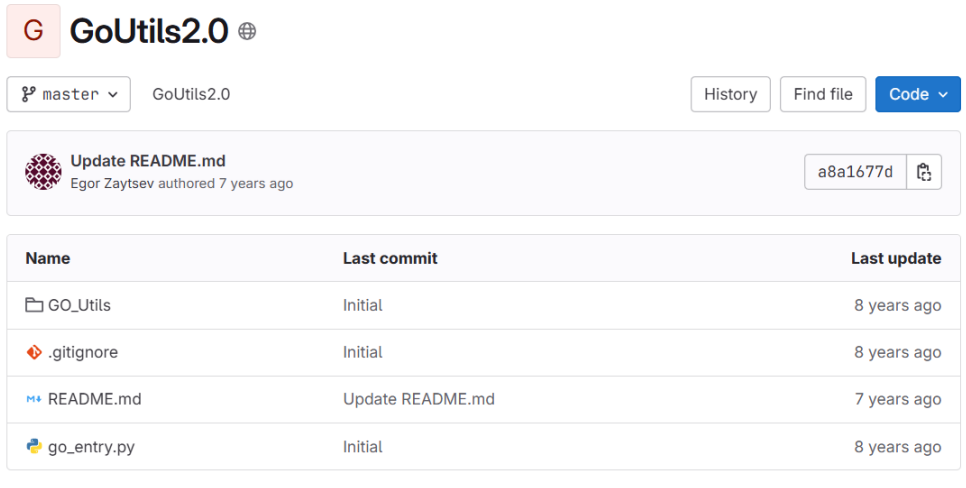


AlphaGolang | A Step-by-Step Go Malware Reversing Methodology for IDA Pro

JUAN ANDRÉS GUERRERO-SAADE / OCTOBER 21, 2021

Genetic Malware Analysis for Golang

Written by **Intezer** - 20 November 2019



Research on dealing with Golang Malware

CASE STUDY : FALL OF TREND

SECRITE | Quick Heal

2024-11-04 17:36	a62cef6dc0e8e55806184...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 17:26	3bd7660e77cbac4a9c8e...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 17:11	e73d0a5c7b43c9109708...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 16:26	b0d15ae15ddea91eba49...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 16:16	35808f69f5f76ddd48c26...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 16:16	e57cfb75a9ebe94ae0d63...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:56	85c0c57eed2a9c08b0091...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:56	e1e42011155b6a06f0620...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:46	63e389a3d5251cbeaaab...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:26	f0b064eb06f164b0d61e6...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:22	4b159ac65cfa47d511af5...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:16	a7e8c3992382bc855aaf2...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:16	d815fe9c20106fa19135d...	elf	Kaiji	elf kaiji	abuse_ch	
2024-11-04 15:16	0b3a333c1f4c6802a71f9...	elf	Kaiji	elf kaiji	abuse_ch	

Community based YARA Rules on Golang Malware. Huge thanks to Abuse.ch!

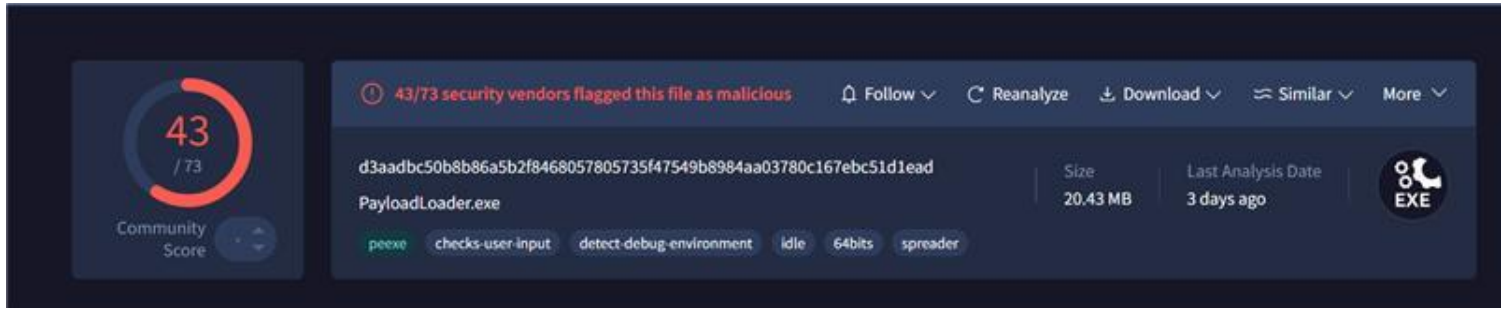
2024-11-07 12:44	181149cbea8570220cfb6...	exe	GOStealer	exe GOStealer	JAMESWT_MHT	
2024-11-07 02:19	f2ecabc649b7db40d38a8...	exe		exe	SecuriteInfoCom	
2024-11-06 15:41	e78fc7300dea3f82b9fb7...	exe	GOBackdoor	exe GOBackdoor	abuse_ch	

CASE STUDY : FALL OF TREND

Claim: Operator Errors Facilitating Proactive Defense.

“The quick adoption of Golang Malware among developers has also led to mistakes like giving away too much artefacts along with the malware implants along with which TAs heavily abuse open source repositories, which already are monitored by Anti-Malware Vendors ”

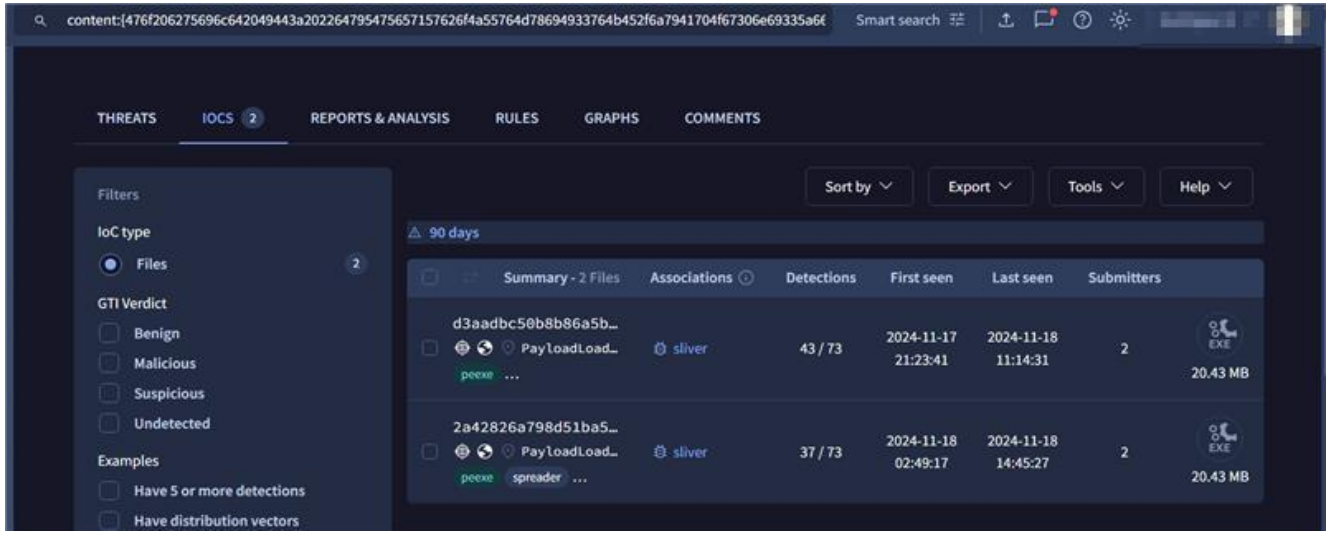
CASE STUDY : FALL OF TREND



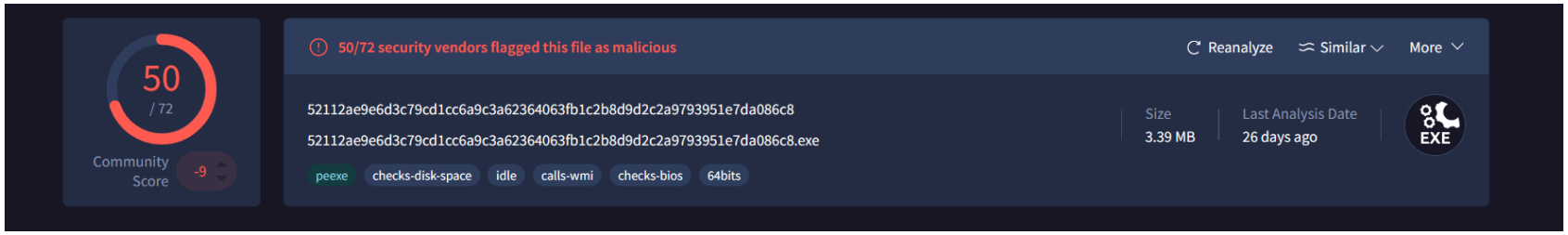

```
Go build ID: "dyTueqWboJUvMxiI3vKE/jyApOg0ni3Zf0vxx-mwq/oMx9oDAgxMj3jW4x-a3W/4c-BObbGpuaSVMhmhkp0"
```

Example 1:

Go-build ID Extracted leads to more payloads part of a simple Sliver C2 campaign.

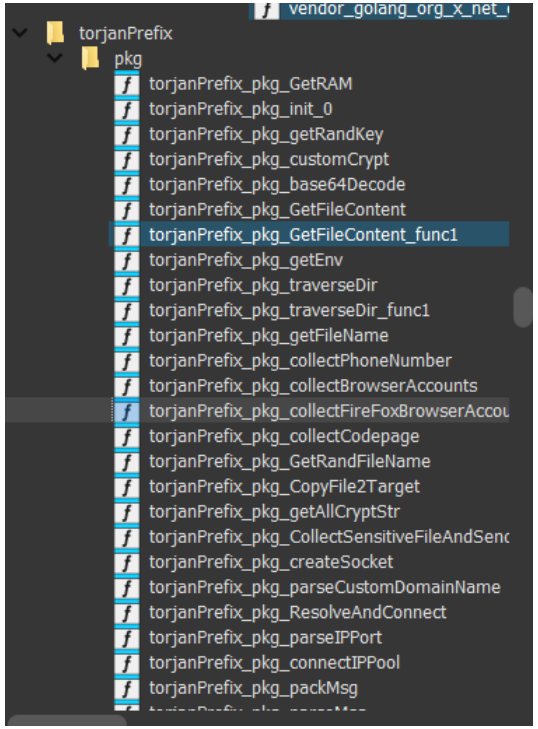


CASE STUDY : FALL OF TREND



Example 2:

Recently discovered unknown Infostealer by hunting specific libraries using VT Hunt.



CASE STUDY : FALL OF TREND

Example 2:

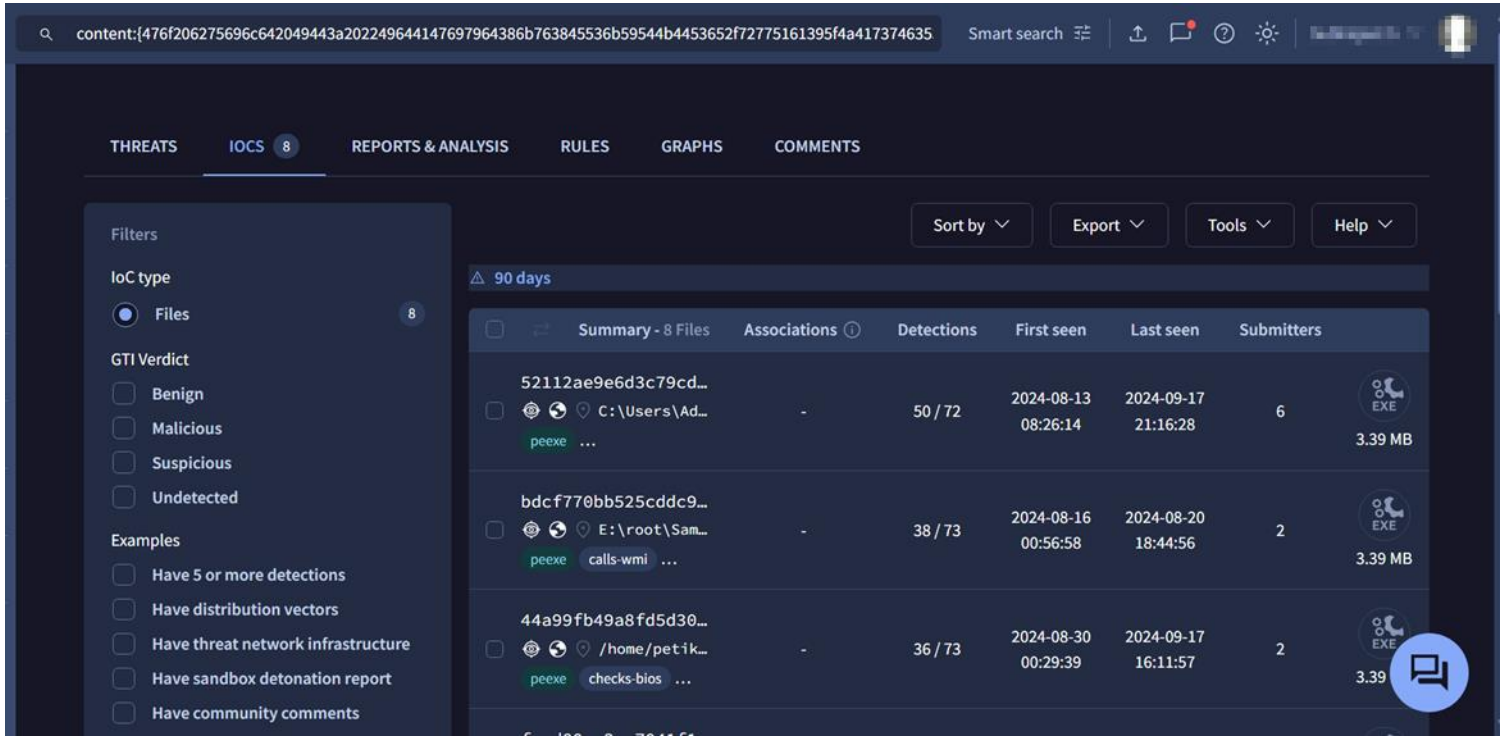
The Go-Build ID is present inside the malware binary.

```
Go build ID: "IdAGiyd8kv8ESkYTKDSe/rwQa9_JAstcSXt8R30Jy/NKkEZtFC-Hl9DyYgKSzl/46pcxpPXq_eLuOQtNGwq"
```

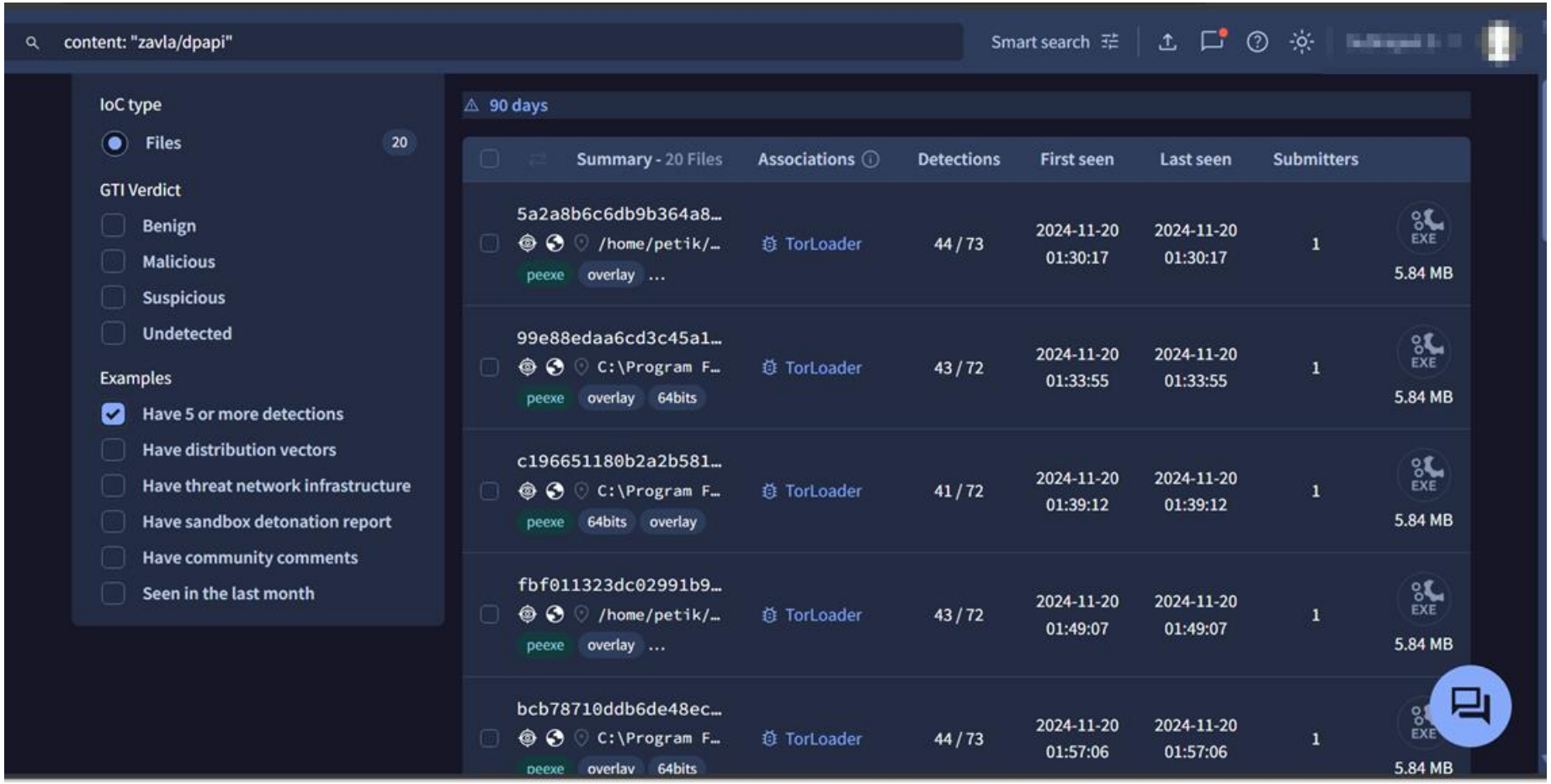
CASE STUDY : FALL OF TREND

Example 2:

The Go-Build ID leads to other samples ITW.

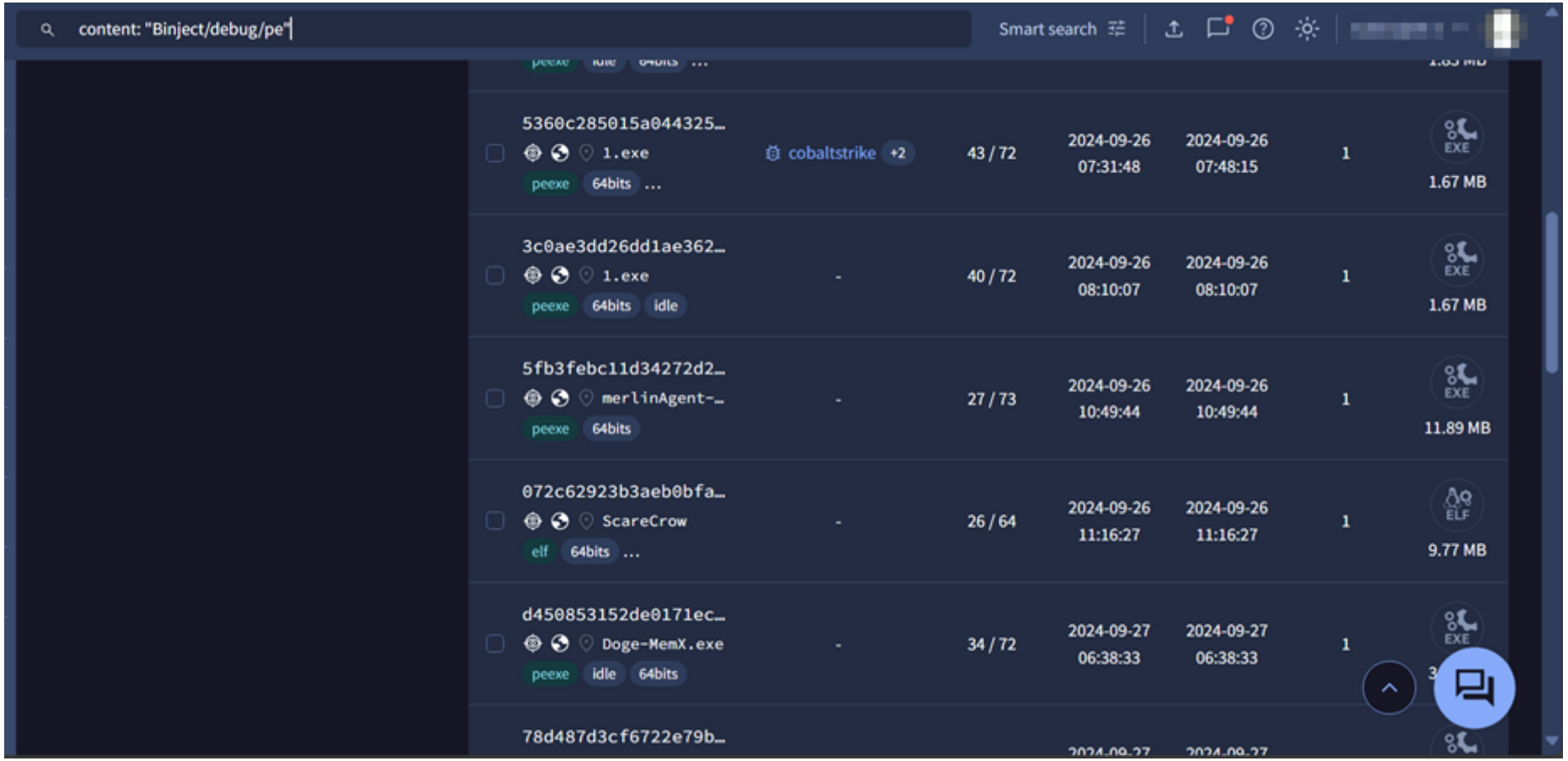


CASE STUDY : FALL OF TREND



Some overused libraries, in Golang malware.

CASE STUDY : FALL OF TREND



Some overused libraries, in Golang malware.

CASE STUDY : PSEUDO RISE

CASE STUDY : PSEUDO-RISE

CLAIMS/HYPOTHESES FOR "PSEUDO-RISE"

- Abuse of Obfuscation Tools.
- Looking into Obfuscation Tools.
- Increased Detection Rates.

CASE STUDY : PSEUDO-RISE

Claim: Abuse of Obfuscation Tools.

"The quick adoption of Golang Malware among developers has also led to mistakes like giving away too much artefacts along with the malware implants lead TAs shift to obfuscators and anti-analysis measures such as Gobfuscator, Garble and many such tools giving them a sense of pseudo-rise."

CASE STUDY : PSEUDO-RISE

SEQRITE | Quick Heal

Obfuscation

When it comes to obfuscation, various tactics make Blackrota difficult to analyze and detect. For one, the malware uses gobfuscate, an open-source tool for Go code, to obfuscate the source code before compiling. It hides various elements of Go source code with random character substitutions – including the package names, global variable names, function names, type names and method names.

"With thousands of random string-named functions and a large number of randomly-named data types, methods and global variables, we could not be sure what third-party Go packages were used inside the sample, making the reverse-analysis almost impossible to move forward," said researchers.

MetaStealer Obfuscated Go Executable

The main executable in MetaStealer bundles is an Intel x86 Mach-O containing compiled and heavily obfuscated Go source code. The Go Build ID has been stripped and function names obfuscated. The obfuscation method bears similarity to that used in obfuscated Sliver and Poseidon malware binaries, and may be a product of the garble obfuscator or similar.

GoRed analysis

Before we proceed to analyzing the current version of **GoRed,** we will provide a retrospective analysis of its evolution.

Versions we found

All the versions we found are shown in the table below.

Version	Description
0.0.1	▪ Assumed to be the first one. ▪ Collects information about the victim. ▪ Source obfuscated with **garble.**

RansomHub and Knight compared

Both payloads are written in Go and most variants of each family are obfuscated with Gobfuscate. Only some early versions of Knight are not obfuscated.

The degree of code overlap between the two families is significant, making it very difficult to differentiate between them. In many cases, a determination could only be confirmed by checking the embedded link to the data leak site.

Snake Ransomware (or EKANS Ransomware) is a Golang ransomware which in the past has affected several companies such as Enel and Honda. The MD5 hashing of the analyzed sample is ED3C05BDE9F0EA0F1321355B03AC42D0 [5]. This sample in particular is obfuscated with Gobfuscate [4], an open source obfuscation project available on Github.

CASE STUDY : PSEUDO-RISE

Claim: Looking into Obfuscation tools.

"We will look into some of the artefacts of these obfuscation tools like Gobfuscator and Garble."

CASE STUDY : PSEUDO-RISE

README BSD-2-Clause license

gobfuscate

When you compile a Go binary, it contains a lot of information about your source code: field names, strings, package paths, etc. If you want to ship a binary without leaking this kind of information, what are you to do?

With gobfuscate, you can compile a Go binary from obfuscated source code. This makes a lot of information difficult or impossible to decipher from the binary.

We will lurk into some of the interesting artefacts of this tool and what happens behind the scenes.

CASE STUDY : PSEUDO-RISE

About : Some interesting features.

- Winhide : This feature could help a binary to run without a GUI or Window, can let the binary to slowly run in the background.
- Obfuscate Package Names: This feature helps the final Go binary to obfuscate the package names excluding the CGO libraries.
- Obfuscate Strings: This feature helps the final Go binary to be generated with obfuscated string names excluding the CGO with a random XOR mask.
- Obfuscate Symbols : This feature helps the final Go binary to be generated with obfuscated string names by directory walking and AST to find top level methods, functions and hashing it with a random seed provided by the user.

CASE STUDY : PSEUDO-RISE

garble

```
go install mvdan.cc/garble@latest
```

Obfuscate Go code by wrapping the Go toolchain. Requires Go 1.23 or later.

```
garble build [build flags] [packages]
```

The tool also supports `garble test` to run tests with obfuscated code, `garble run` to obfuscate and execute simple programs, and `garble reverse` to de-obfuscate text such as stack traces. Run `garble -h` to see all available commands and flags.

You can also use `go install mvdan.cc/garble@master` to install the latest development version.

We will lurk into some of the interesting artefacts of this tool and what happens behind the scenes.

CASE STUDY : PSEUDO-RISE

About : Some interesting features.

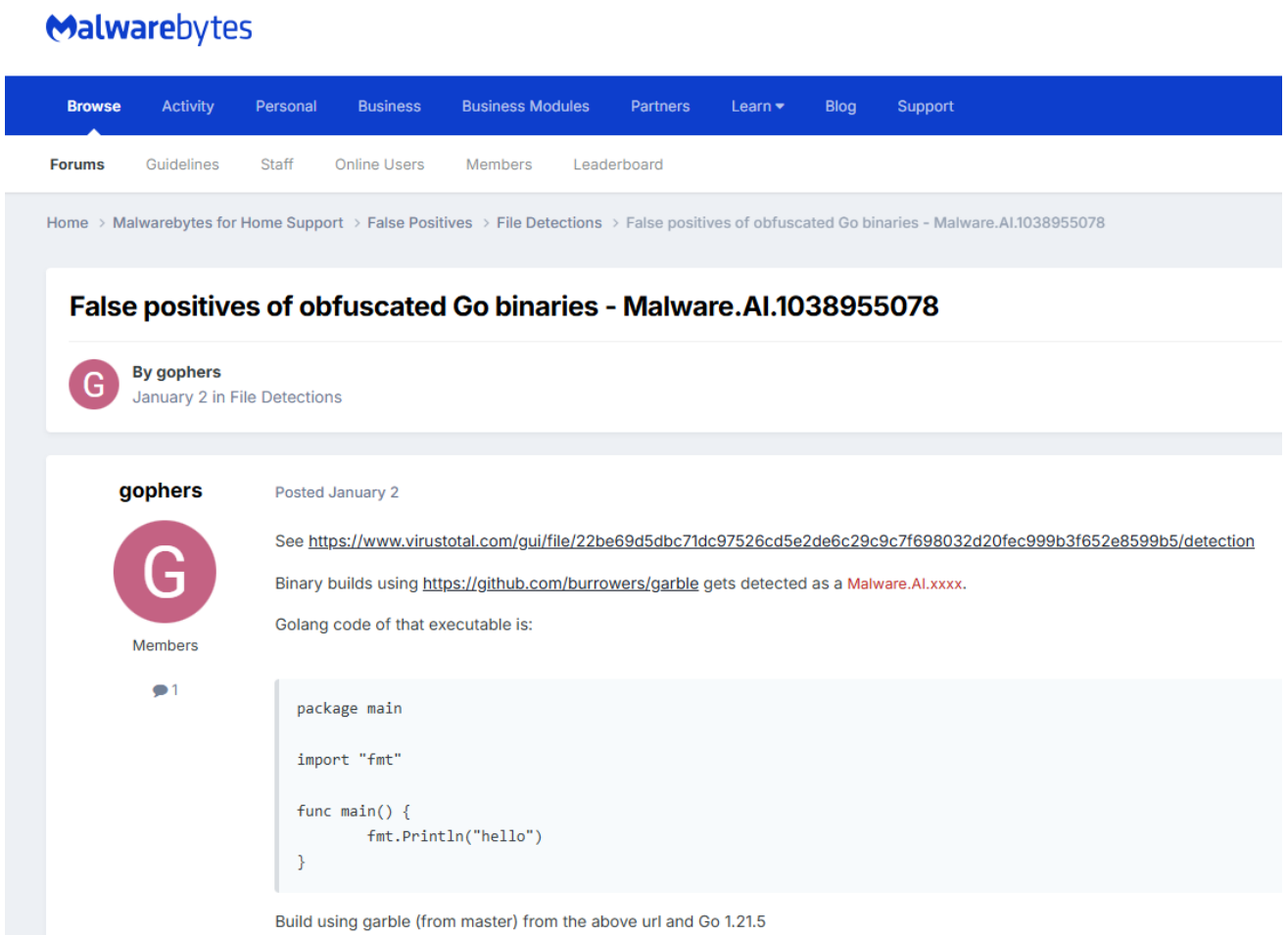
- Control Flow Obfuscation : This feature adds bunch of junk code in the obfuscated binary using Garble.
- Obfuscate Package Names: This feature helps the final Go binary to obfuscate the package names excluding the CGO libraries.
- Obfuscate Strings: This feature helps the final Go binary to be generated with obfuscated string names excluding the CGO with a random XOR mask and much more like ADD, NOR etc.
- Obfuscate Symbols : This feature helps the final Go binary to be generated with obfuscated string names by directory walking and AST to find top level methods, functions and hashing it with a random seed provided by the user.
- Go-Toolchain Integration : Hooks into the Go-Toolchain seamlessly using –toolexec , ensuring compatibility with existing build pipeline and tools.
- Anti-Analysis : Garble employs bunch of anti-analysis techniques which including removing various headers which contain important info.

CASE STUDY : PSEUDO-RISE

Claim: Increased Detection Rate.

"The quick adoption of these obfuscators and packers by threat actors and groups have let anti-malware vendors to heavily flag and block these and leading to increased detection rates."

CASE STUDY : PSEUDO-RISE



Malwarebytes

Browse Activity Personal Business Business Modules Partners Learn Blog Support

Forums Guidelines Staff Online Users Members Leaderboard

Home › Malwarebytes for Home Support › False Positives › File Detections › False positives of obfuscated Go binaries - Malware.AI.1038955078

False positives of obfuscated Go binaries - Malware.AI.1038955078

G **By gophers**
January 2 in File Detections

gophers

G

Members

1

Posted January 2

See https://www.virustotal.com/gui/file/22be69d5dbc71dc97526cd5e2de6c29c9c7f698032d20fec999b3f652e8599b5/detection

Binary builds using https://github.com/burrowers/garble gets detected as a Malware.AI.xxxx.

Golang code of that executable is:

```
package main

import "fmt"

func main() {
        fmt.Println("hello")
}
```

Build using garble (from master) from the above url and Go 1.21.5

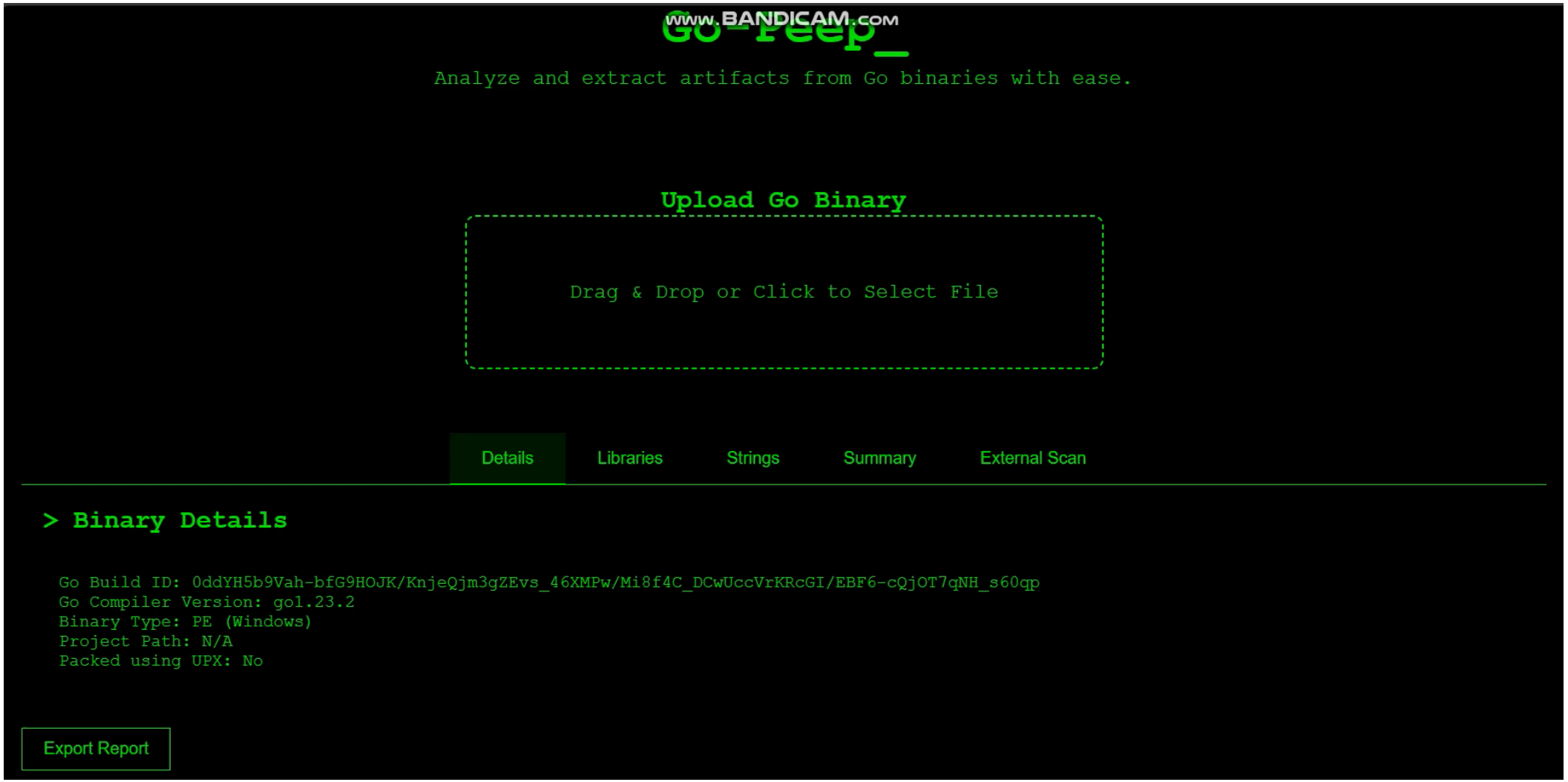
CONCLUSION

CASE STUDY : PSEUDO-RISE

- Detections and blocking on both malicious and non-malicious binaries.
- Threat Actors have taken an alternative route by using different open source packers , obfuscators or their own custom ones.
- A decline in Golang malware scenario as now community support for research against these obfuscators and Golang malware in general is at all time high.
- Peak enthusiasm amongst malware developers to learn Golang.

TOOL-DEMO : GO-PEEP

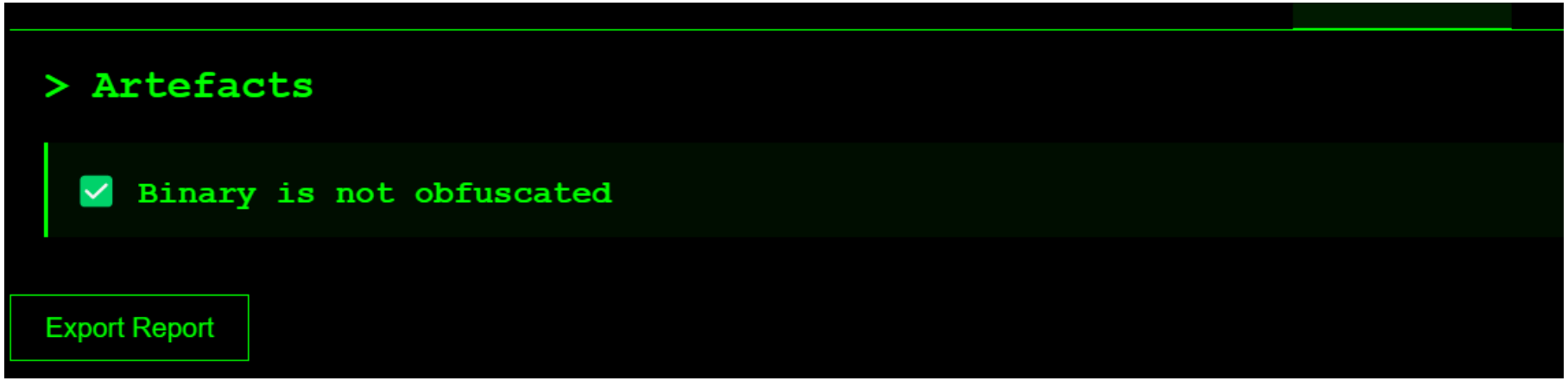
TOOL-DEMO : GO-PEEP

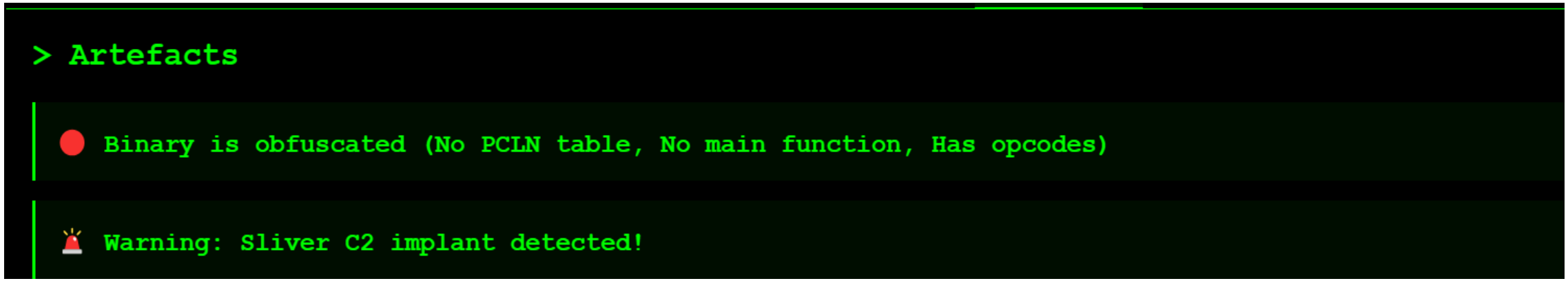


TOOL-DEMO : GO-PEEP

You can find the demo here.

TOOL-DEMO : GO-PEEP





TOOL-DEMO : GO-PEEP

```
Interesting Path: C:/Program Files/Go/src/fmt/format.go

Interesting Path: C:/Users/Pseudo-user/Desktop/Go-Peep/binary/main.go
```

Q &A

Any Questions?

Thank You

Innovate. Simplify. Secure.