Tricks, Treats, and Threats: Cobalt Strike & the Goblin Lurking in Plain Sight

hunt.io/blog/tricks-treats-threats-cobalt-strike-the-goblin-lurking-in-plain-sight

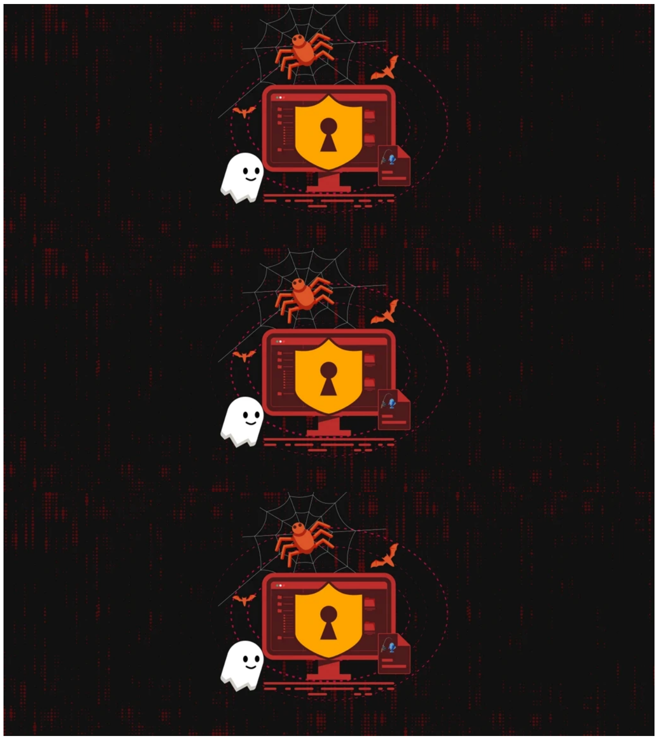


TABLE OF CONTENTS

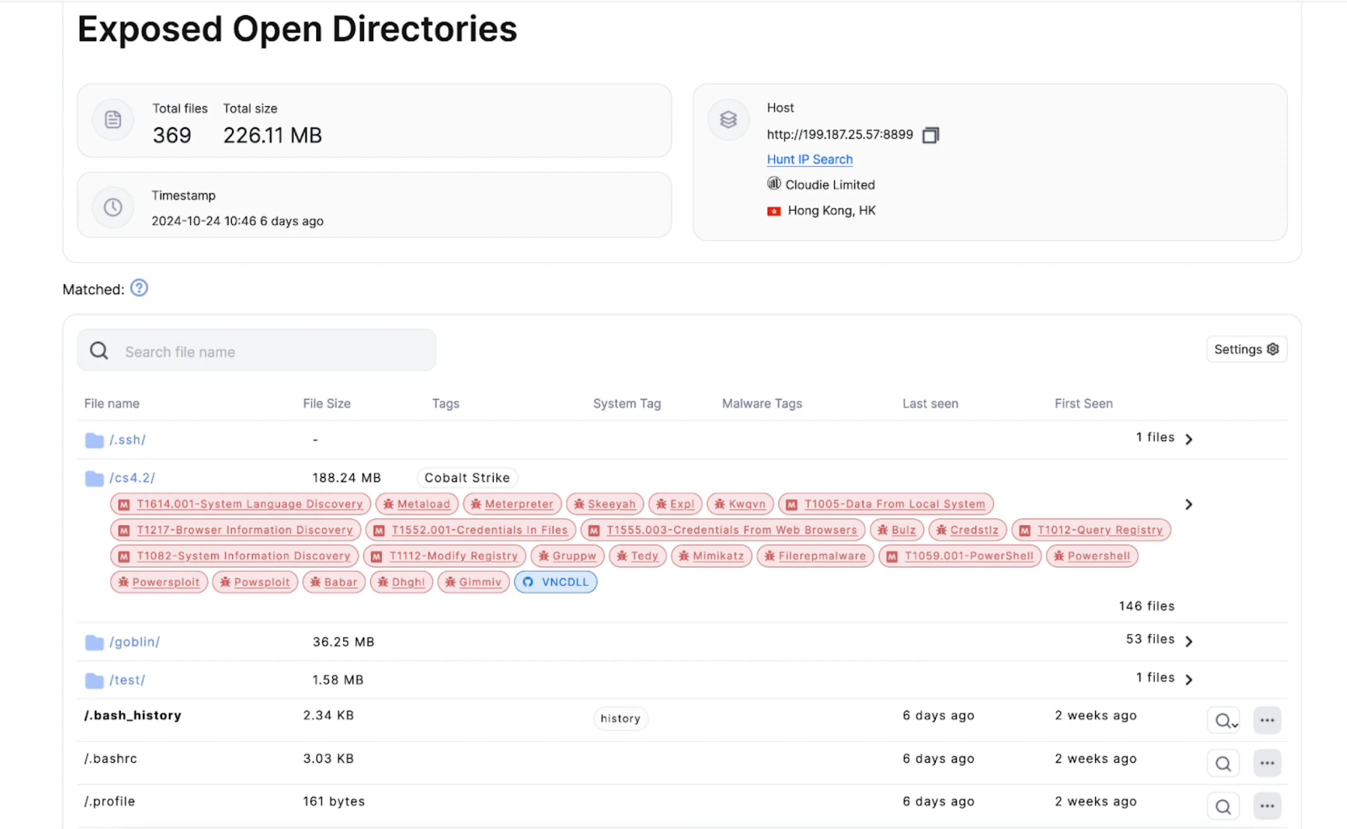
In the spirit of Halloween, a recent open directory discovery offers a curious combination of tools-Cobalt Strike, Goblin, and BrowserGhost. These names may evoke a playful twist, but each represents serious capabilities often leveraged by red teams and adversaries. This collection of sinister tools sits waiting in the open, much like treats left out on Halloween night-but for those who wander into this directory, the tricks are lurking, too.

Summary of Findings:

- An open directory exposed Cobalt Strike 4.2, a widely used post-exploitation framework, exploit code targeting vulnerabilities (CVEs) dating back to 2014.
- BrowserGhost, is a red team tool for extracting saved passwords from web browsers, suggesting a focus on credential theft.
- The open-source Goblin phishing tool possibly used to target Chinese-speaking educational platforms and steal user credentials.

A Curious Encounter: Analyzing the Open Directory

The open directory hosted at 199.187.25[.]57:8899 on Cloudie Limited's ASN in Hong Kong provided a unique glimpse into a collection of tools likely used for malicious purposes. Among the contents was Cobalt Strike version 4.2, released in November 2020, a folder named "goblin," which we'll cover later, and logs capturing command history and output.



Exposed Open Directories

Total files 369

Total size 226.11 MB

Timestamp 2024-10-24 10:46 6 days ago

Host

http://199.187.25.57:8899

Hunt IP Search

Cloudie Limited

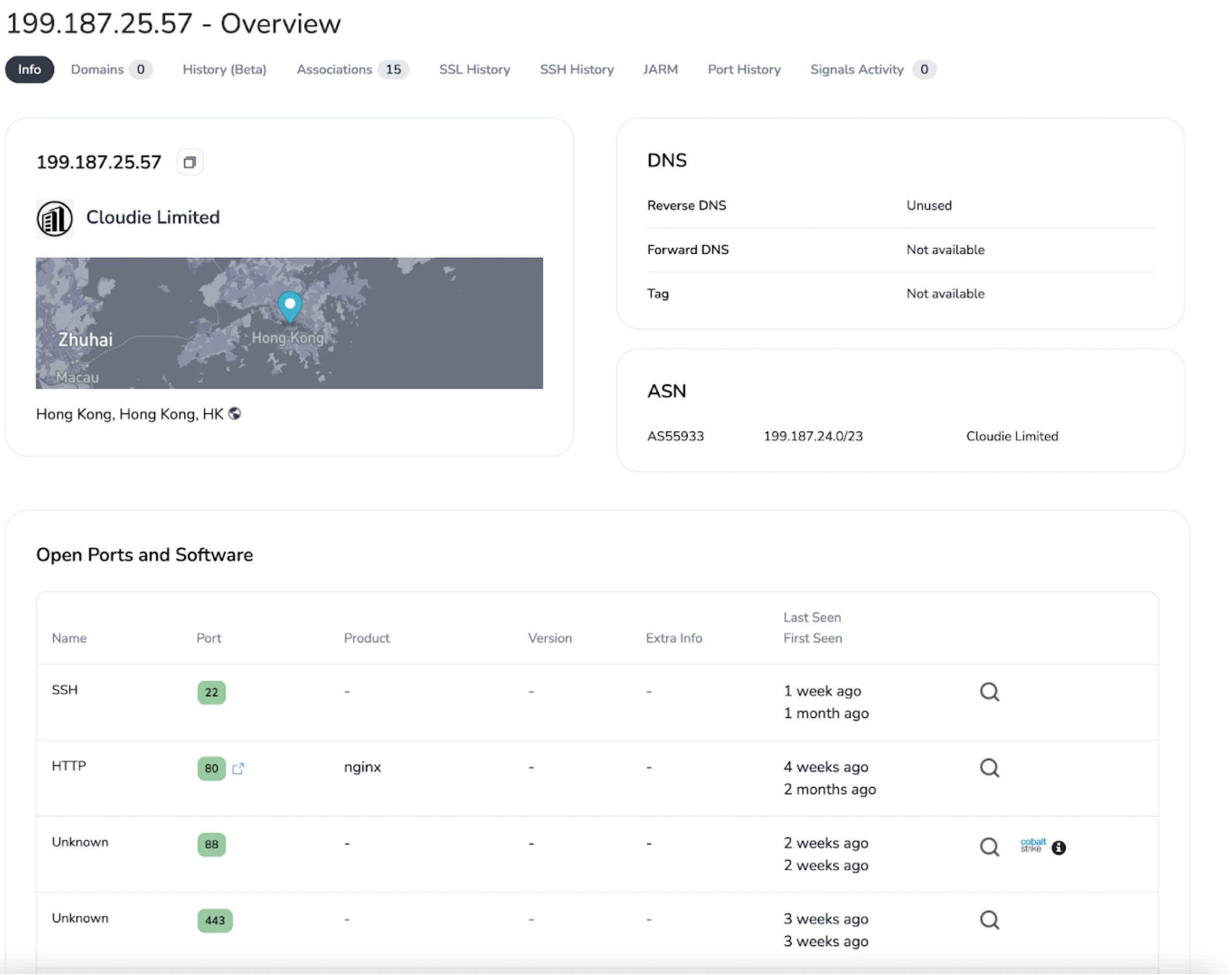
Hong Kong, HK

Matched:

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/.ssh/	-					1 files
/cs4.2/	188.24 MB	Cobalt Strike		T1614.001-System Language Discovery Metaload Meterpreter Skeeyah Expl Kwqvn T1005-Data From Local System T1217-Browser Information Discovery T1552.001-Credentials In Files T1555.003-Credentials From Web Browsers Bulz Credstlz T1012-Query Registry T1082-System Information Discovery T1112-Modify Registry Gruppw Tedy Mimikatz Filerepmalware T1059.001-PowerShell Powershell Powersploit Powsploit Babar Dhghl Gimmiv VNCDLL		146 files
/goblin/	36.25 MB					53 files
/test/	1.58 MB					1 files
/.bash_history	2.34 KB		history		6 days ago	2 weeks ago
/.bashrc	3.03 KB				6 days ago	2 weeks ago
/.profile	161 bytes				6 days ago	2 weeks ago

Figure 1: Screenshot of the open directory page for the server at 199.187.25[.]57 in Hunt

The server, likely running a Linux-based operating system, hosted the directory using Python 3.8.10 SimpleHTTP version 0.6. Beyond the directory contents, Hunt scanners identified several Cobalt Strike team servers on ports **88**, **4343**, and **5555**. An Nginx web server on port 80 responded with a 404 error displaying a "Site Not Found" message in Simplified Chinese.



199.187.25.57 - Overview

199.187.25.57

Cloudie Limited

Hong Kong, Hong Kong, HK

DNS

Reverse DNS	Unused
Forward DNS	Not available
Tag	Not available

ASN

AS55933	199.187.24.0/23	Cloudie Limited

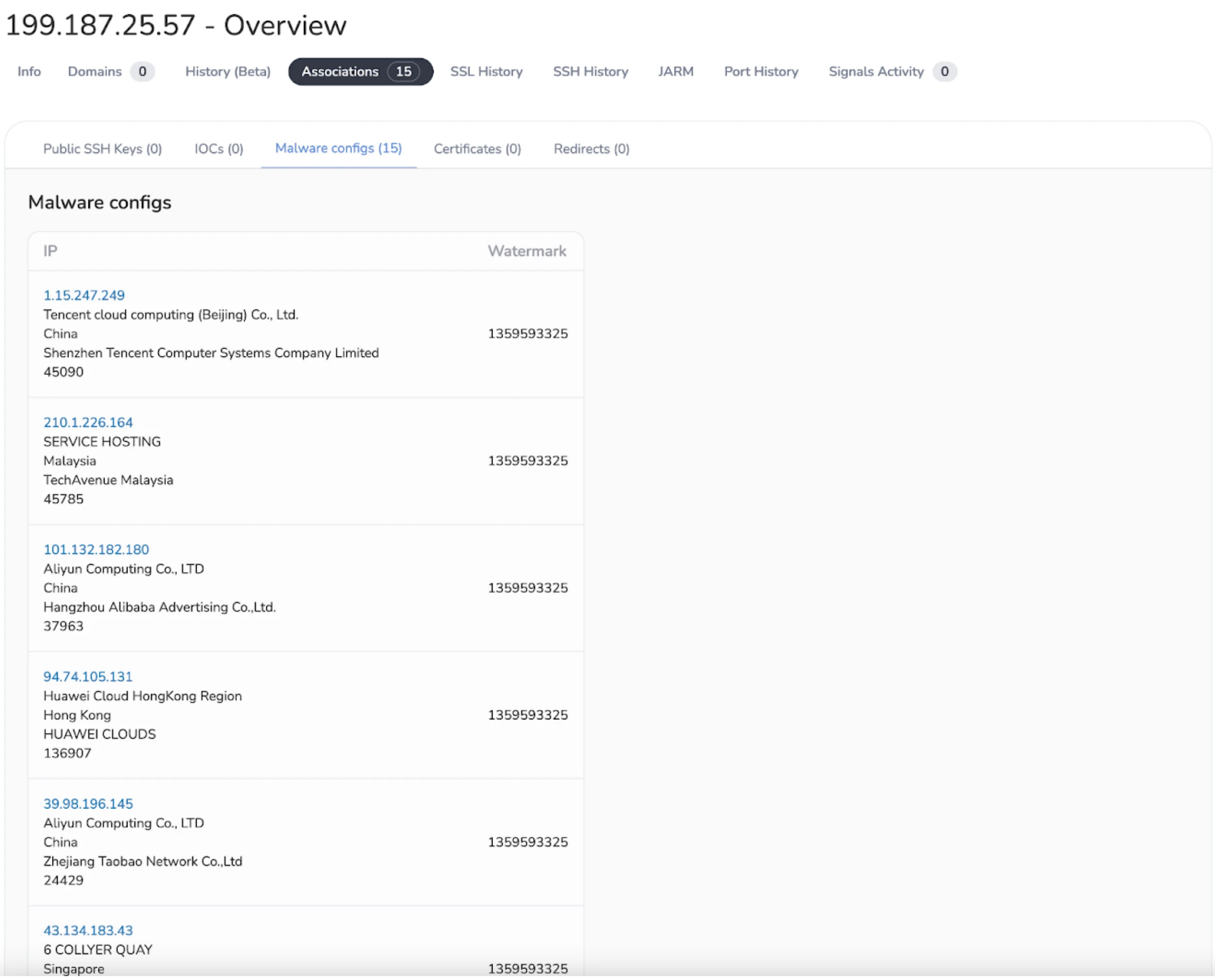
Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
SSH	22	-	-	-	1 week ago 1 month ago	
HTTP	80	nginx	-	-	4 weeks ago 2 months ago	
Unknown	88	-	-	-	2 weeks ago 2 weeks ago	cobalt strike
Unknown	443	-	-	-	3 weeks ago 3 weeks ago	

Figure 2: Overview of the suspicious IP, including ports, domains, and associations in Hunt

Interestingly, the watermark extracted from the beacon configuration (click the "i" button next to the Cobalt Strike symbol), 1359593325, was seen associated with just 15 other servers according to our visibility. Such a small number of servers sharing this unique identifier suggests a distinct but possibly more extensive managed operation.

Nested within the cs4.2 folder were additional payloads targeting historical vulnerabilities like CVE-2014-4113 and CVE-2020-0796, Meterpreter, and web shell payloads-evidence of a comprehensive toolkit geared towards exploitation and persistence.



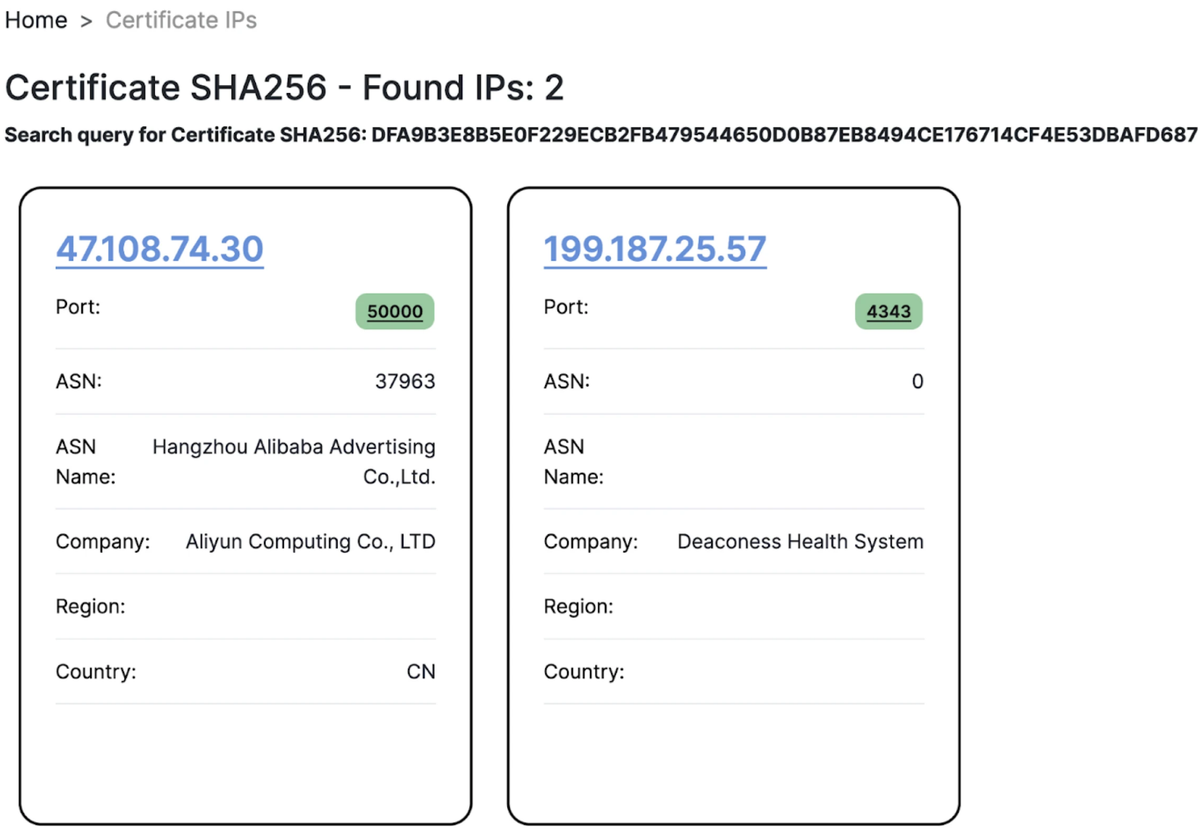
199.187.25.57 - Overview

Malware configs

IP	Watermark
1.15.247.249 Tencent cloud computing (Beijing) Co., Ltd. China Shenzhen Tencent Computer Systems Company Limited 45090	1359593325
210.1.226.164 SERVICE HOSTING Malaysia TechAvenue Malaysia 45785	1359593325
101.132.182.180 Aliyun Computing Co., LTD China Hangzhou Alibaba Advertising Co.,Ltd. 37963	1359593325
94.74.105.131 Huawei Cloud HongKong Region Hong Kong HUAWEI CLOUDS 136907	1359593325
39.98.196.145 Aliyun Computing Co., LTD China Zhejiang Taobao Network Co.,Ltd 24429	1359593325
43.134.183.43 6 COLLYER QUAY Singapore	1359593325

Figure 3: Snippet of the IPs observed sharing the same Cobalt Strike Watermark (Source: Hunt)
*A complete list of all the IP addresses sharing the watermark can be found at the end of this post.

On October 15, this server briefly hosted a well-known Cobalt Strike TLS certificate, SHA-256 hash: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53DBAFD687 for just one day. The only other IP to share this certificate was 47.108.74[.]30, hosted on Aliyun Computing Co. LTD's ASN, indicating potential shared infrastructure or coordination between two servers/actors.



Home > Certificate IPs

Certificate SHA256 - Found IPs: 2

Search query for Certificate SHA256: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53DBAFD687

47.108.74.30

Port:	50000
ASN:	37963
ASN Name:	Hangzhou Alibaba Advertising Co.,Ltd.
Company:	Aliyun Computing Co., LTD
Region:	
Country:	CN

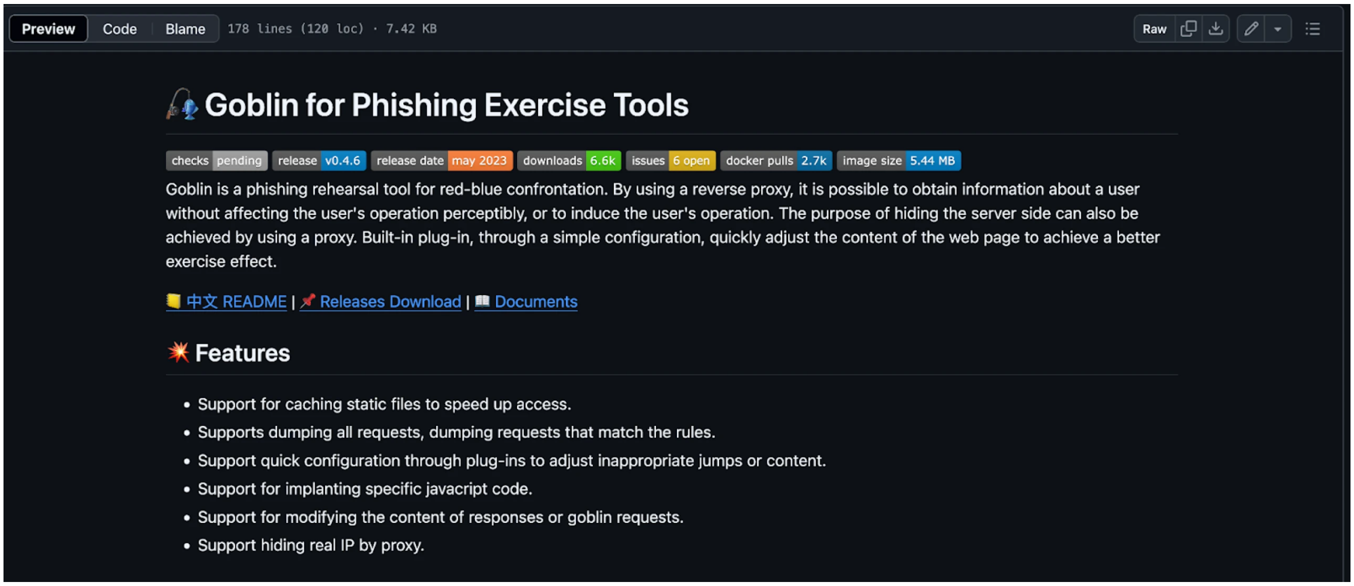
199.187.25.57

Port:	4343
ASN:	0
ASN Name:	
Company:	Deaconess Health System
Region:	
Country:	

Figure 4: Screenshot of IPs sharing the same certificate (Source: Hunt)

Goblin's Tricks: Phishing with a Purpose

The Goblin phishing tool, as described in its GitHub project overview, serves as a platform for red and blue team exercises. Goblin operates by proxying traffic to mimic user interactions while remaining unobtrusive, allowing for an authentic simulation of phishing attempts. Its customizable plug-ins and support for embedded JavaScript make it adaptable for legitimate training scenarios and potential malicious use.



Goblin for Phishing Exercise Tools

Goblin is a phishing rehearsal tool for red-blue confrontation. By using a reverse proxy, it is possible to obtain information about a user without affecting the user's operation perceptibly, or to induce the user's operation. The purpose of hiding the server side can also be achieved by using a proxy. Built-in plug-in, through a simple configuration, quickly adjust the content of the web page to achieve a better exercise effect.

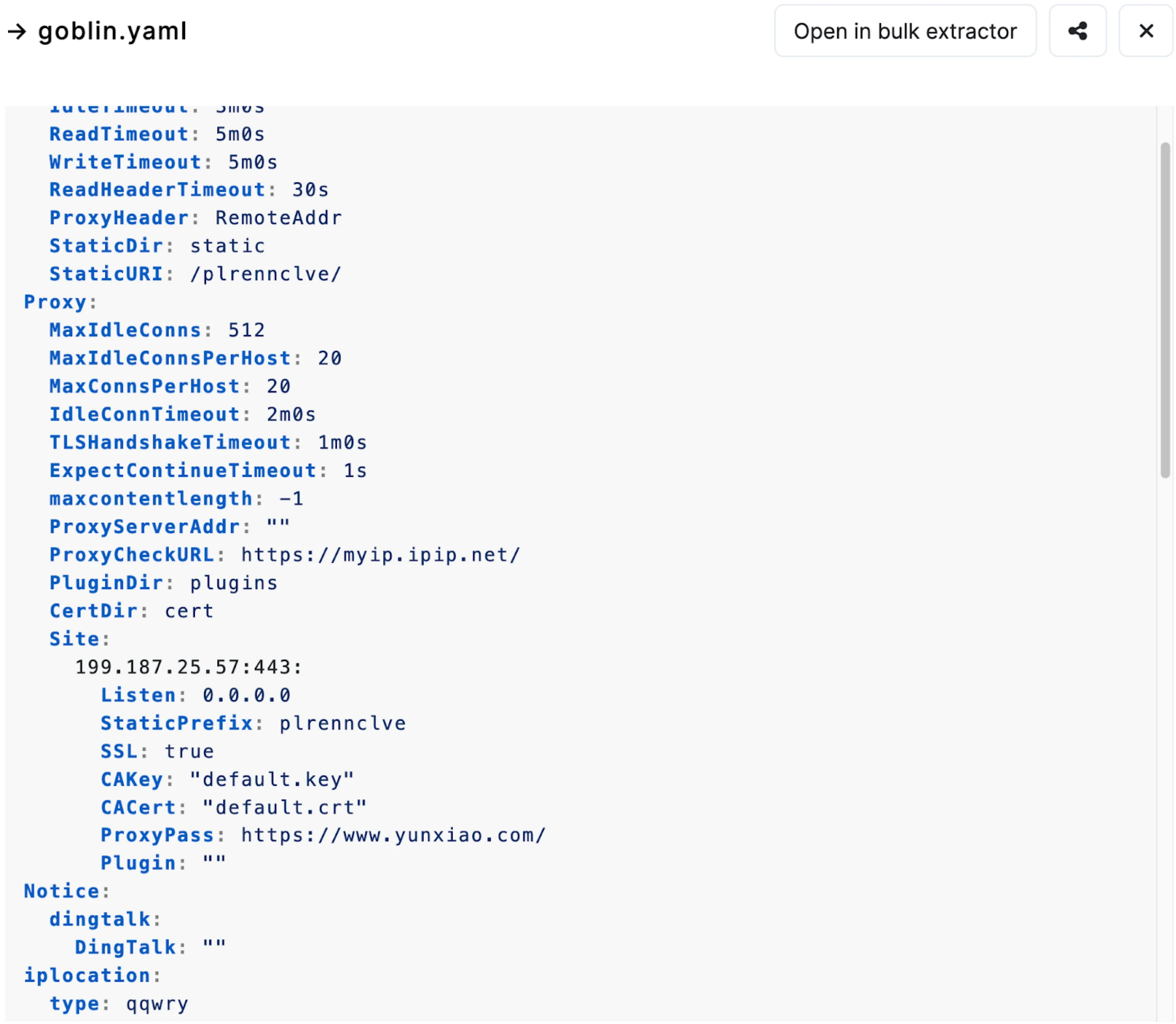
中文 README | Releases Download | Documents

Features

- Support for caching static files to speed up access.
- Supports dumping all requests, dumping requests that match the rules.
- Support quick configuration through plug-ins to adjust inappropriate jumps or content.
- Support for implanting specific javacript code.
- Support for modifying the content of responses or goblin requests.
- Support hiding real IP by proxy.

Figure 4: Screenshot of the English-language README version of the Goblin Project (Source: GitHub)

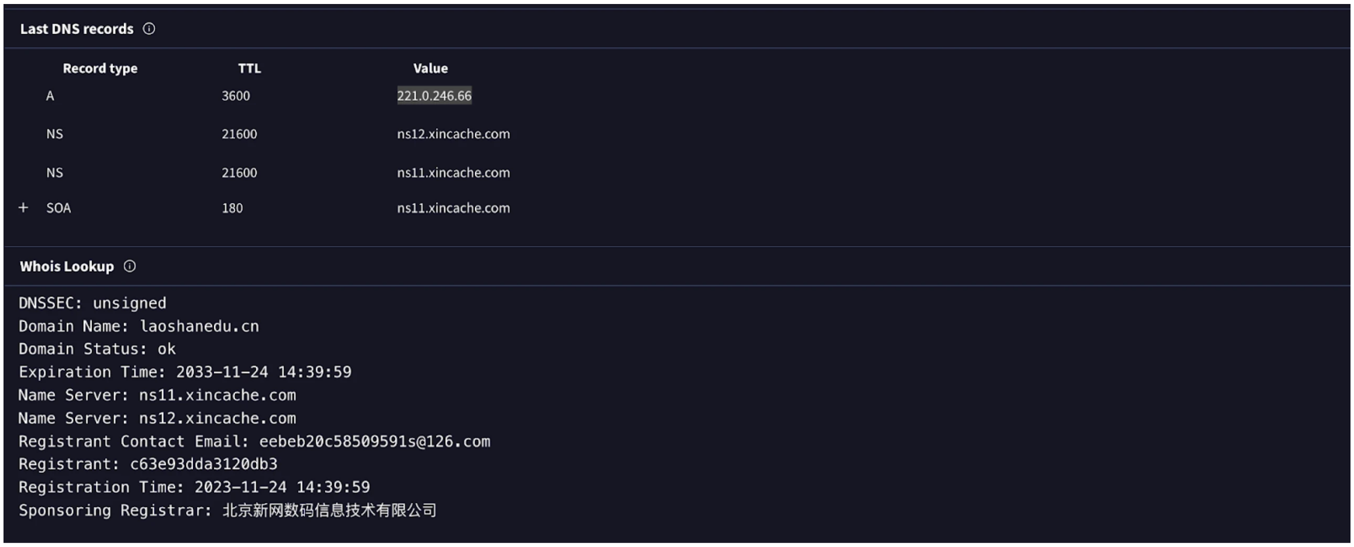
A review of Goblin's YAML configuration file in the directory reveals that the operator has configured traffic to proxy through yunxiao[.]com, a domain associated with Alibaba Cloud's Yunxiao DevOps platform, and laoshanedu.cn. While the purpose behind this setup remains unclear, our analysis failed to reveal any injected JavaScript or identifiable phishing targets.



```
  IdleTimeout: 5m0s
  ReadTimeout: 5m0s
  WriteTimeout: 5m0s
  ReadHeaderTimeout: 30s
  ProxyHeader: RemoteAddr
  StaticDir: static
  StaticURI: /plrennclve/
Proxy:
  MaxIdleConns: 512
  MaxIdleConnsPerHost: 20
  MaxConnsPerHost: 20
  IdleConnTimeout: 2m0s
  TLSHandshakeTimeout: 1m0s
  ExpectContinueTimeout: 1s
  maxcontentlength: -1
  ProxyServerAddr: ""
  ProxyCheckURL: https://myip.ipip.net/
  PluginDir: plugins
  CertDir: cert
  Site:
    199.187.25.57:443:
      Listen: 0.0.0.0
      StaticPrefix: plrennclve
      SSL: true
      CAKey: "default.key"
      CACert: "default.crt"
      ProxyPass: https://www.yunxiao.com/
      Plugin: ""
Notice:
  dingtalk:
    DingTalk: ""
iplocation:
  type: qqwry
```

Figure 5: Snippet of the Goblin YAML config file from the Hunt open directory page

Further analysis revealed that laoshanedu[.]cn was registered in November 2023 with Beijing Xinnet Digital Information Technology Co., Ltd. and used nameservers from xincache[.]com. Using an education-based naming format and recent setup suggests the domain may serve as a plausible cover for Goblin, potentially mimicking an educational institution.



Last DNS records ⓘ

	Record type	TTL	Value
	A	3600	221.0.246.66
	NS	21600	ns12.xincache.com
	NS	21600	ns11.xincache.com
+	SOA	180	ns11.xincache.com

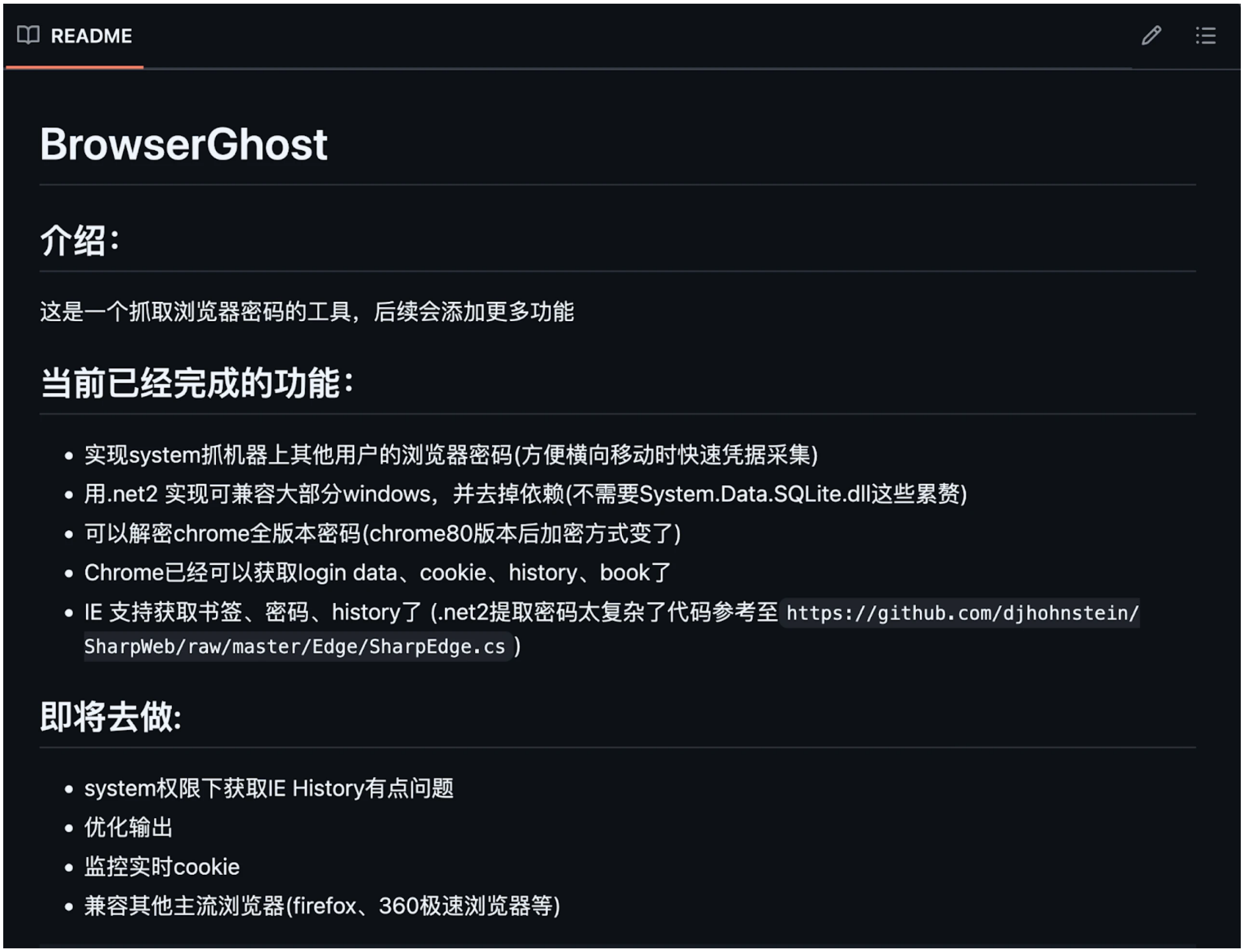
Whois Lookup ⓘ

```
DNSSEC: unsigned
Domain Name: laoshanedu.cn
Domain Status: ok
Expiration Time: 2033-11-24 14:39:59
Name Server: ns11.xincache.com
Name Server: ns12.xincache.com
Registrant Contact Email: eebeb20c58509591s@126.com
Registrant: c63e93dda3120db3
Registration Time: 2023-11-24 14:39:59
Sponsoring Registrar: 北京新网数码信息技术有限公司
```

Figure 6: DNS & WhoIs records in VirusTotal for laoshanedu[.]cn

BrowserGhost: A Phantom's Approach to Credential Access

The final tool we'll examine, BrowserGhost, is another open-source utility, this time found within the Cobalt Strike folder, designed to extract stored passwords from popular web browsers, including Chrome, Firefox, 360 Extreme, and Edge.



README

BrowserGhost

介绍：

这是一个抓取浏览器密码的工具，后续会添加更多功能

当前已经完成的功能：

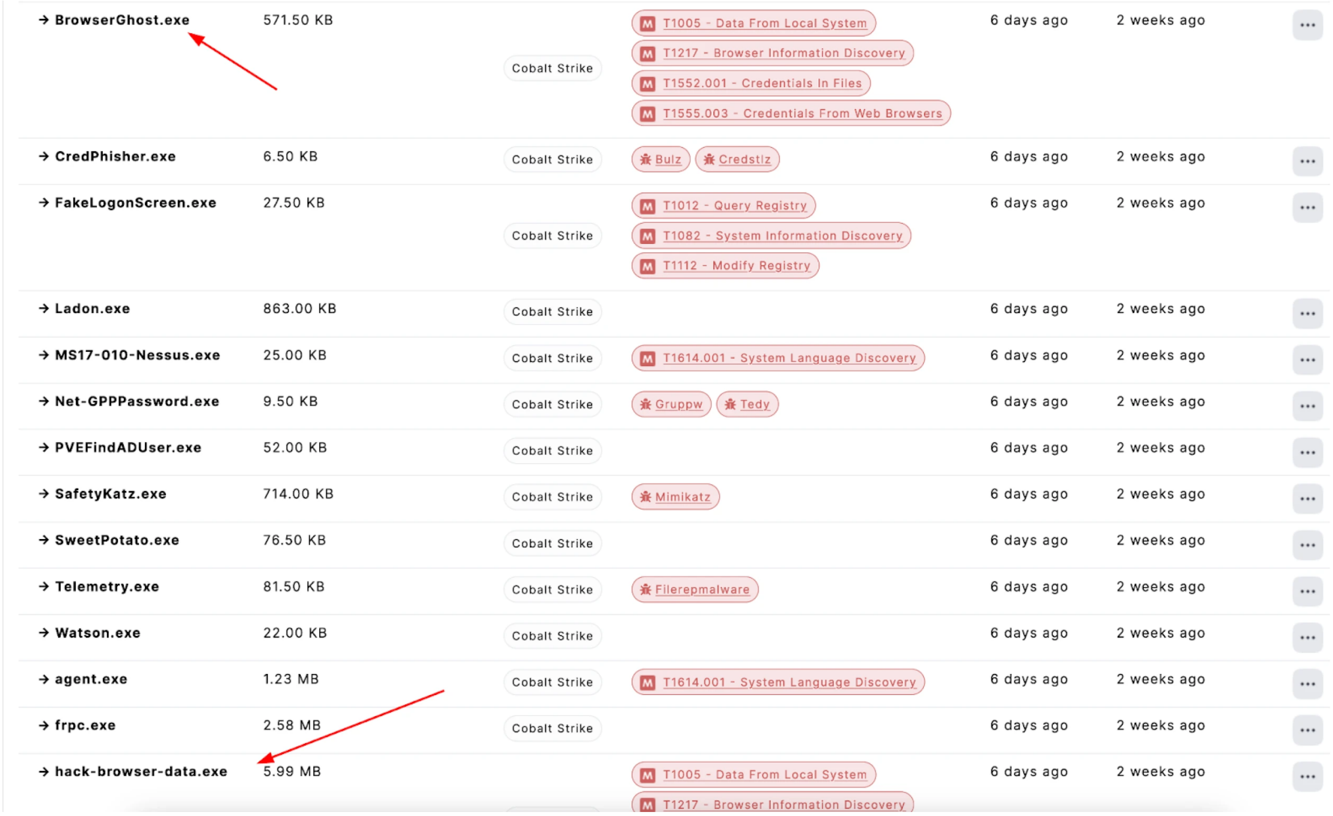
- 实现system抓机器上其他用户的浏览器密码(方便横向移动时快速凭据采集)
- 用.net2 实现可兼容大部分windows，并去掉依赖(不需要System.Data.SQLite.dll这些累赘)
- 可以解密chrome全版本密码(chrome80版本后加密方式变了)
- Chrome已经可以获取login data、cookie、history、book了
- IE 支持获取书签、密码、history了 (.net2提取密码太复杂了代码参考至 `https://github.com/djhohnstein/SharpWeb/raw/master/Edge/SharpEdge.cs`)

即将去做:

- system权限下获取IE History有点问题
- 优化输出
- 监控实时cookie
- 兼容其他主流浏览器(firefox、360极速浏览器等)

Figure 7: Screenshot of the BrowserGhost README in GitHub

Alongside BrowserGhost, the directory also contained HackBrowserData, a tool specifically built to extract and decrypt sensitive browser information. This combination of tools hints at an operator with a strong interest in harvesting browser-stored credentials, signaling a well-equipped red team or an adversary with a clear focus on data exfiltration from compromised systems.



→ BrowserGhost.exe	571.50 KB	Cobalt Strike	T1005 - Data From Local System T1217 - Browser Information Discovery T1552.001 - Credentials In Files T1555.003 - Credentials From Web Browsers	6 days ago	2 weeks ago
→ CredPhisher.exe	6.50 KB	Cobalt Strike	Bulz Credstiz	6 days ago	2 weeks ago
→ FakeLogonScreen.exe	27.50 KB	Cobalt Strike	T1012 - Query Registry T1082 - System Information Discovery T1112 - Modify Registry	6 days ago	2 weeks ago
→ Ladon.exe	863.00 KB	Cobalt Strike		6 days ago	2 weeks ago
→ MS17-010-Nessus.exe	25.00 KB	Cobalt Strike	T1614.001 - System Language Discovery	6 days ago	2 weeks ago
→ Net-GPPPassword.exe	9.50 KB	Cobalt Strike	Gruppw Tedy	6 days ago	2 weeks ago
→ PVEFindADUser.exe	52.00 KB	Cobalt Strike		6 days ago	2 weeks ago
→ SafetyKatz.exe	714.00 KB	Cobalt Strike	Mimikatz	6 days ago	2 weeks ago
→ SweetPotato.exe	76.50 KB	Cobalt Strike		6 days ago	2 weeks ago
→ Telemetry.exe	81.50 KB	Cobalt Strike	Filerepmalware	6 days ago	2 weeks ago
→ Watson.exe	22.00 KB	Cobalt Strike		6 days ago	2 weeks ago
→ agent.exe	1.23 MB	Cobalt Strike	T1614.001 - System Language Discovery	6 days ago	2 weeks ago
→ frpc.exe	2.58 MB	Cobalt Strike		6 days ago	2 weeks ago
→ hack-browser-data.exe	5.99 MB		T1005 - Data From Local System T1217 - Browser Information Discovery	6 days ago	2 weeks ago

Figure 8: Screenshot of multiple files within the cs4.2 folder, including BrowserGhost and HackBrowserData

Closing the Door on a Haunted Directory

In wrapping up our Halloween dive into this open directory, we've highlighted tools like Cobalt Strike, Goblin, and BrowserGhost—each with capabilities that extend from red teaming to potentially darker uses. Our findings highlight how such tools, although often seen in professional settings, can be used for more sinister purposes—a reminder of the treats and tricks still hidden within the cybersecurity threat landscape.

If you want to learn more about these spooky threats and light your Jack-o-lantern against their tricks, get in touch with Hunt.io!

Open Directory Observables

IP Address	Hosting Country	ASN	Cobalt Strike Watermark
1199.187.25[.]57:8899	HK	Cloudie Limited	1359593325

Shared Certificate (Major Cobalt Strike)

IP Address	Hosting Country	ASN	Domain(s)	Certificate
47.108.74[.]30	CN	Hangzhou Alibaba Advertising Co.,Ltd.	tbc.cbshscs.comtom[.]cn cbshscs.comtom[.]cn file.cbshscs.comtom[.]cn	Common Name: Major Cobalt Strike Country: Earth Org: cobaltstrike OrgUnit: AdvancedPenTesting City: Somewhere State: Cyberspace SHA-256 Hash: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53I

Cobalt Strike Watermark (1359593325) Overlaps

IP Address	Hosting Country	ASN	Domain(s)
43.134.183.43	HK	Tencent Building, Kejizhongyi Avenue	N/A
101.132.182.180	CN	Hangzhou Alibaba Advertising Co.,Ltd.	N/A

IP Address	Hosting Country	ASN	Domain(s)
106.15.40[.]123	CN	Hangzhou Alibaba Advertising Co.,Ltd.	N/A
39.98.196[.]145	CN	Zhejiang Taobao Network Co.,Ltd	N/A
94.74.105[.]131	HK	HUAWEI CLOUDS	N/A
1.15.247[.]249	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
1.117.72[.]154	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
27.102.118[.]70	SK	DAOU TECHNOLOGY	ns1.kjdfklha[.]top ns2.kjdfklha[.]top kjdfklha[.]top blog.kjdfklha[.]top
210.1.226.[.]164	MA	TechAvenue Malaysia	N/A
101.43.157[.]20	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
106.52.236[.]88	CN	Shenzhen Tencent Computer Systems Company Limited	src.idvfecx.qiniudns[.]com
111.231.140[.]197	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
124.221.167[.]192	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
117.72.10[.]22	CN	Beijing Jingdong 360 Degree E-commerce Co., Ltd.	dn2ufncur4f3f[.]shop
119.3.153[.]81	CN	Huawei Cloud Service data center	N/A

TABLE OF CONTENTS

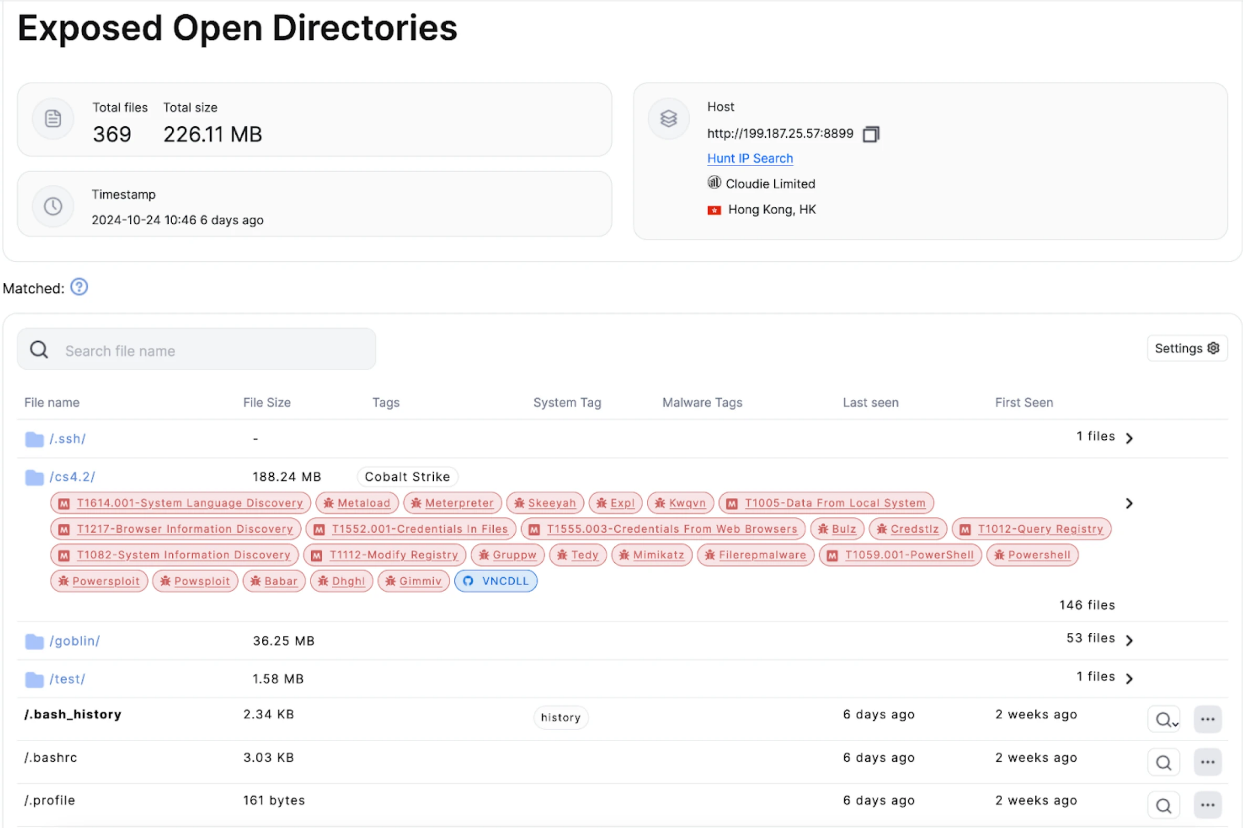
In the spirit of Halloween, a recent open directory discovery offers a curious combination of tools-Cobalt Strike, Goblin, and BrowserGhost. These names may evoke a playful twist, but each represents serious capabilities often leveraged by red teams and adversaries. This collection of sinister tools sits waiting in the open, much like treats left out on Halloween night-but for those who wander into this directory, the tricks are lurking, too.

Summary of Findings:

- An open directory exposed Cobalt Strike 4.2, a widely used post-exploitation framework, exploit code targeting vulnerabilities (CVEs) dating back to 2014.
- BrowserGhost, is a red team tool for extracting saved passwords from web browsers, suggesting a focus on credential theft.
- The open-source Goblin phishing tool possibly used to target Chinese-speaking educational platforms and steal user credentials.

A Curious Encounter: Analyzing the Open Directory

The open directory hosted at 199.187.25[.]57:8899 on Cloudie Limited's ASN in Hong Kong provided a unique glimpse into a collection of tools likely used for malicious purposes. Among the contents was Cobalt Strike version 4.2, released in November 2020, a folder named "goblin," which we'll cover later, and logs capturing command history and output.



Exposed Open Directories

Total files 369

Total size 226.11 MB

Timestamp 2024-10-24 10:46 6 days ago

Host http://199.187.25.57:8899

Hunt IP Search

Cloudie Limited

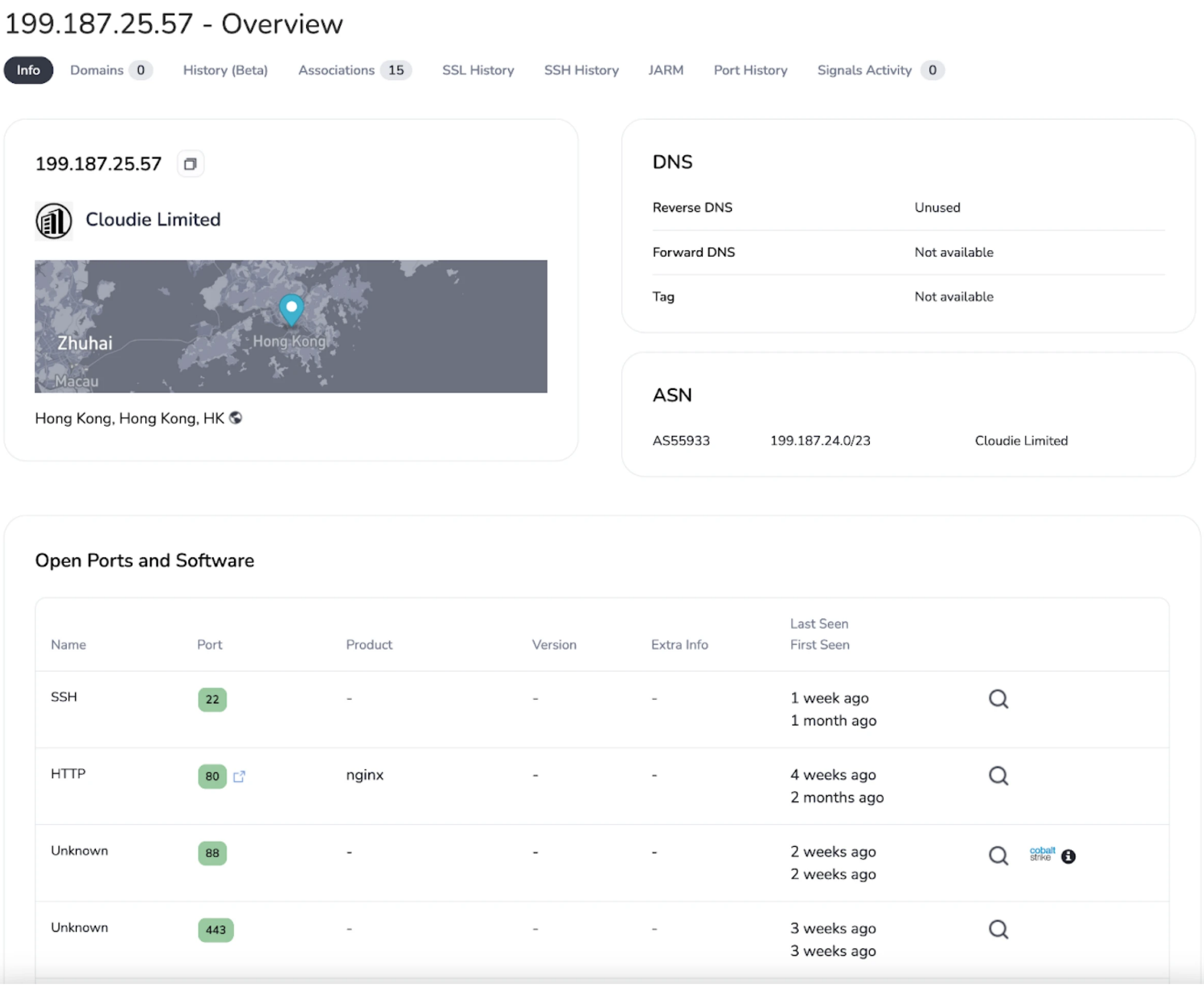
Hong Kong, HK

Matched:

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen
/.ssh/	-					1 files
/cs4.2/	188.24 MB	Cobalt Strike T1614.001-System Language Discovery Metaload Meterpreter Skeeyah Expl Kwqvn T1005-Data From Local System T1217-Browser Information Discovery T1552.001-Credentials In Files T1555.003-Credentials From Web Browsers Bulz Credstlz T1012-Query Registry T1082-System Information Discovery T1112-Modify Registry Gruppw Tedy Mimikatz Filerepmalware T1059.001-PowerShell Powershell Powersploit Powsploit Babar Dhghl Gimmiv VNCDLL				146 files
/goblin/	36.25 MB					53 files
/test/	1.58 MB					1 files
/.bash_history	2.34 KB		history		6 days ago	2 weeks ago
/.bashrc	3.03 KB				6 days ago	2 weeks ago
/.profile	161 bytes				6 days ago	2 weeks ago

Figure 1: Screenshot of the open directory page for the server at 199.187.25[.]57 in Hunt

The server, likely running a Linux-based operating system, hosted the directory using Python 3.8.10 SimpleHTTP version 0.6. Beyond the directory contents, Hunt scanners identified several Cobalt Strike team servers on ports **88**, **4343**, and **5555**. An Nginx web server on port 80 responded with a 404 error displaying a "Site Not Found" message in Simplified Chinese.



199.187.25.57 - Overview

199.187.25.57

Cloudie Limited

Hong Kong, Hong Kong, HK

DNS

Reverse DNS	Unused
Forward DNS	Not available
Tag	Not available

ASN

AS55933	199.187.24.0/23	Cloudie Limited

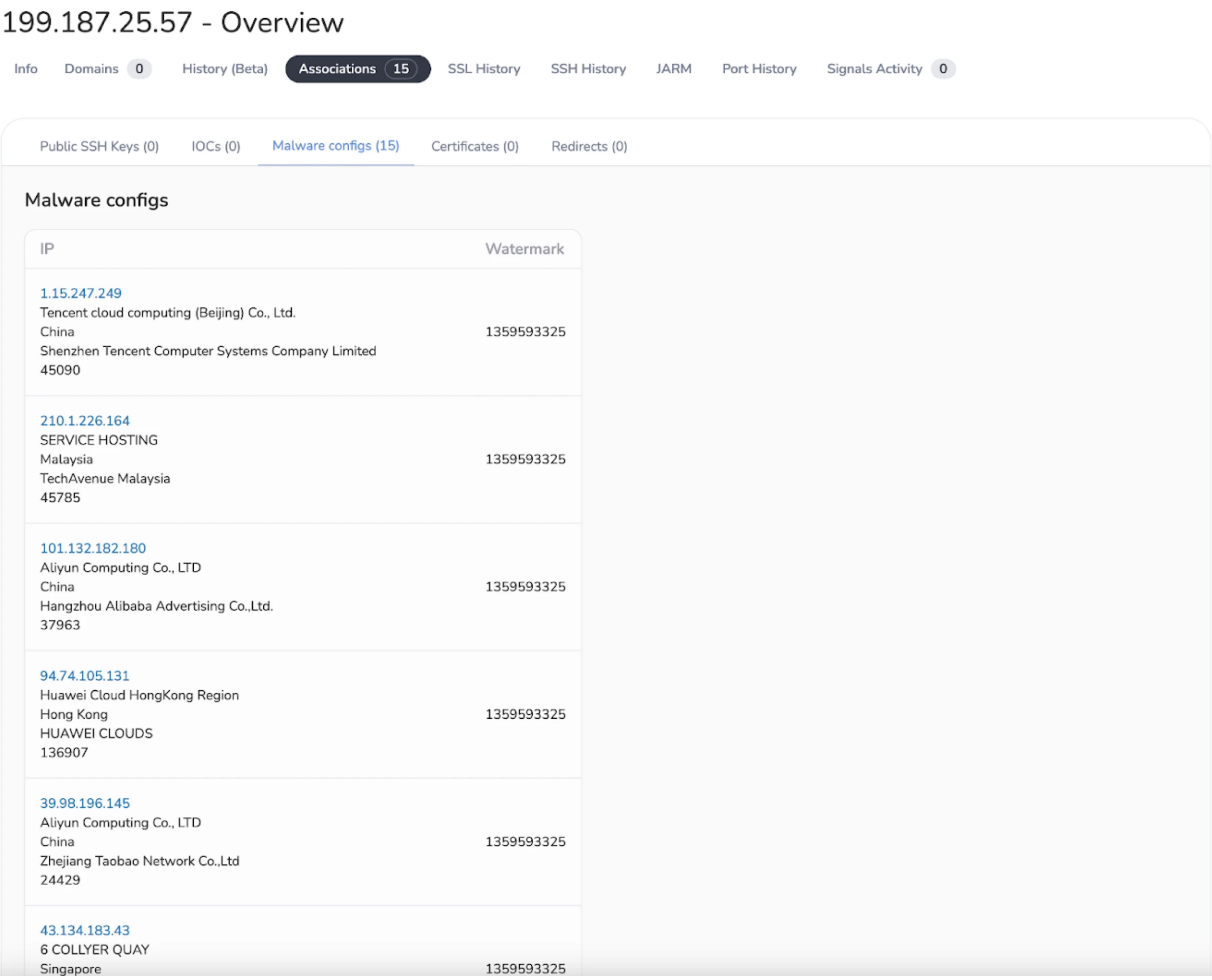
Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
SSH	22	-	-	-	1 week ago 1 month ago	
HTTP	80	nginx	-	-	4 weeks ago 2 months ago	
Unknown	88	-	-	-	2 weeks ago 2 weeks ago	cobalt strike
Unknown	443	-	-	-	3 weeks ago 3 weeks ago	

Figure 2: Overview of the suspicious IP, including ports, domains, and associations in Hunt

Interestingly, the watermark extracted from the beacon configuration (click the "i" button next to the Cobalt Strike symbol), 1359593325, was seen associated with just 15 other servers according to our visibility. Such a small number of servers sharing this unique identifier suggests a distinct but possibly more extensive managed operation.

Nested within the cs4.2 folder were additional payloads targeting historical vulnerabilities like CVE-2014-4113 and CVE-2020-0796, Meterpreter, and web shell payloads-evidence of a comprehensive toolkit geared towards exploitation and persistence.

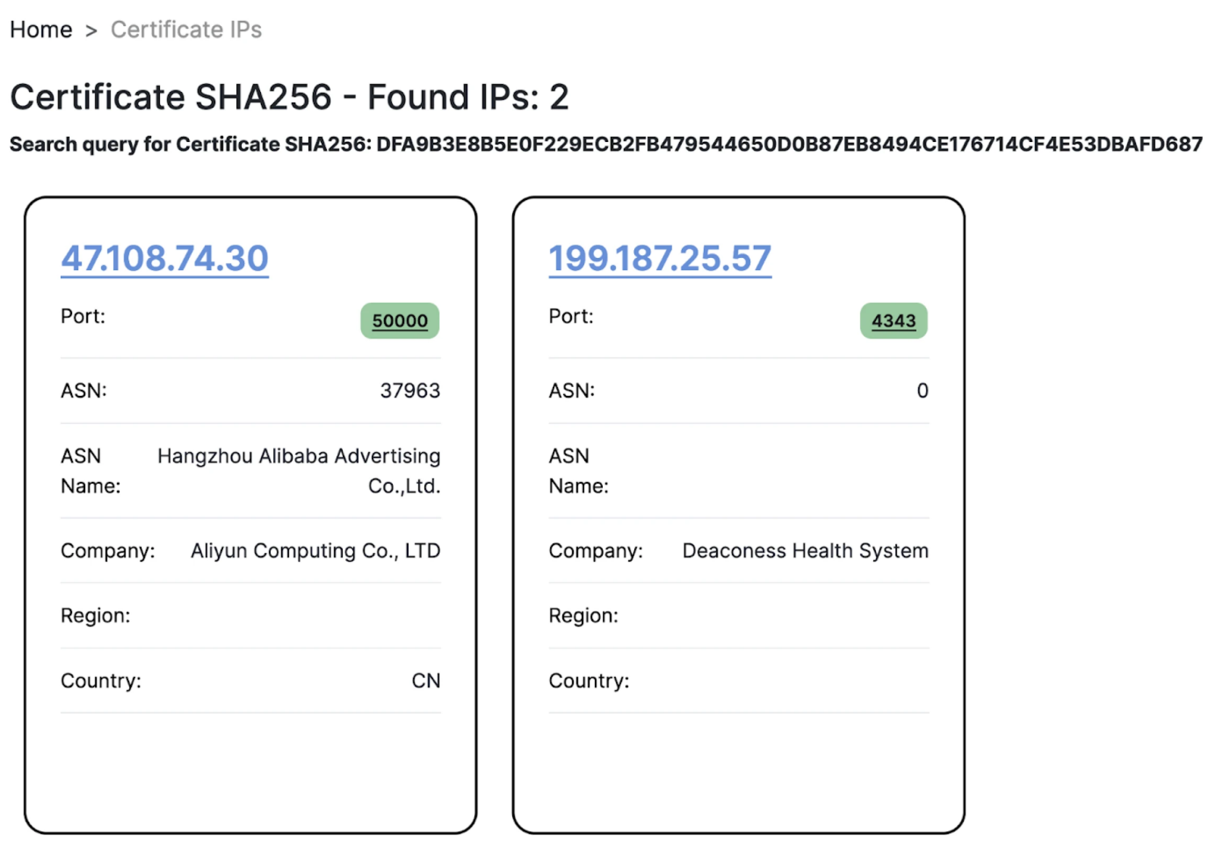


Malware configs

IP	Watermark
1.15.247.249 Tencent cloud computing (Beijing) Co., Ltd. China Shenzhen Tencent Computer Systems Company Limited 45090	1359593325
210.1.226.164 SERVICE HOSTING Malaysia TechAvenue Malaysia 45785	1359593325
101.132.182.180 Aliyun Computing Co., LTD China Hangzhou Alibaba Advertising Co.,Ltd. 37963	1359593325
94.74.105.131 Huawei Cloud HongKong Region Hong Kong HUAWEI CLOUDS 136907	1359593325
39.98.196.145 Aliyun Computing Co., LTD China Zhejiang Taobao Network Co.,Ltd 24429	1359593325
43.134.183.43 6 COLLYER QUAY Singapore	1359593325

Figure 3: Snippet of the IPs observed sharing the same Cobalt Strike Watermark (Source: Hunt)
*A complete list of all the IP addresses sharing the watermark can be found at the end of this post.

On October 15, this server briefly hosted a well-known Cobalt Strike TLS certificate, SHA-256 hash: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53DBAFD687 for just one day. The only other IP to share this certificate was 47.108.74[.]30, hosted on Aliyun Computing Co. LTD's ASN, indicating potential shared infrastructure or coordination between two servers/actors.



Home > Certificate IPs

Certificate SHA256 - Found IPs: 2

Search query for Certificate SHA256: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53DBAFD687

47.108.74.30

Port:	50000
ASN:	37963
ASN Name:	Hangzhou Alibaba Advertising Co.,Ltd.
Company:	Aliyun Computing Co., LTD
Region:	
Country:	CN

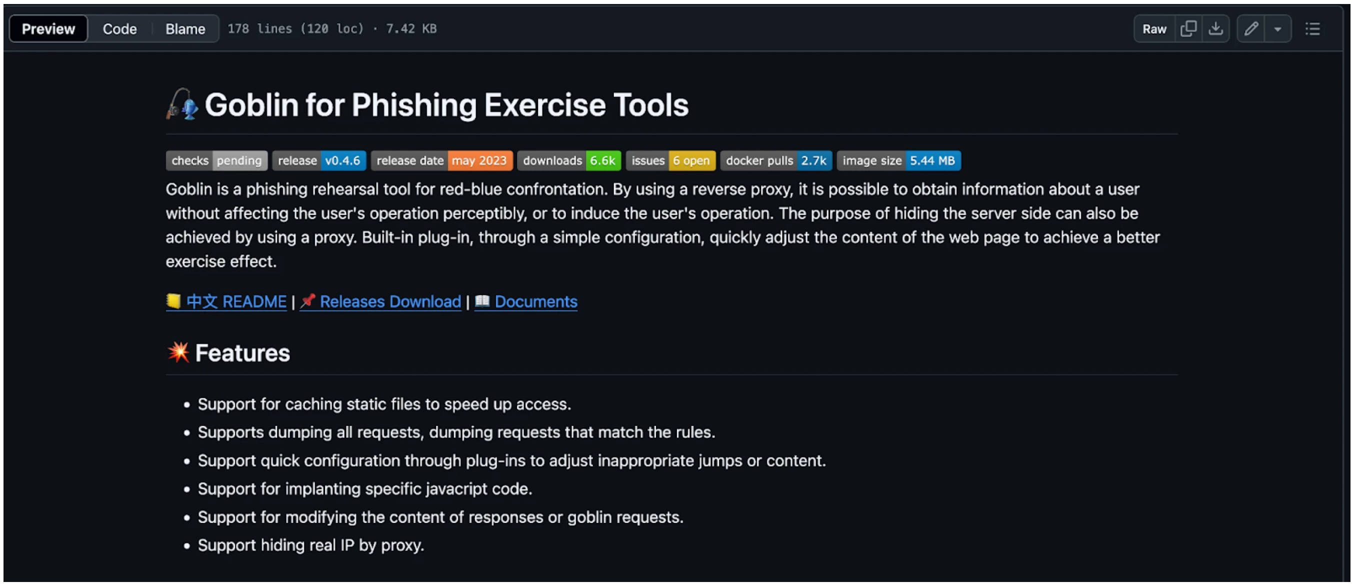
199.187.25.57

Port:	4343
ASN:	0
ASN Name:	
Company:	Deaconess Health System
Region:	
Country:	

Figure 4: Screenshot of IPs sharing the same certificate (Source: Hunt)

Goblin's Tricks: Phishing with a Purpose

The Goblin phishing tool, as described in its GitHub project overview, serves as a platform for red and blue team exercises. Goblin operates by proxying traffic to mimic user interactions while remaining unobtrusive, allowing for an authentic simulation of phishing attempts. Its customizable plug-ins and support for embedded JavaScript make it adaptable for legitimate training scenarios and potential malicious use.



Goblin for Phishing Exercise Tools

checks pending | release v0.4.6 | release date may 2023 | downloads 6.6k | issues 6 open | docker pulls 2.7k | image size 5.44 MB

Goblin is a phishing rehearsal tool for red-blue confrontation. By using a reverse proxy, it is possible to obtain information about a user without affecting the user's operation perceptibly, or to induce the user's operation. The purpose of hiding the server side can also be achieved by using a proxy. Built-in plug-in, through a simple configuration, quickly adjust the content of the web page to achieve a better exercise effect.

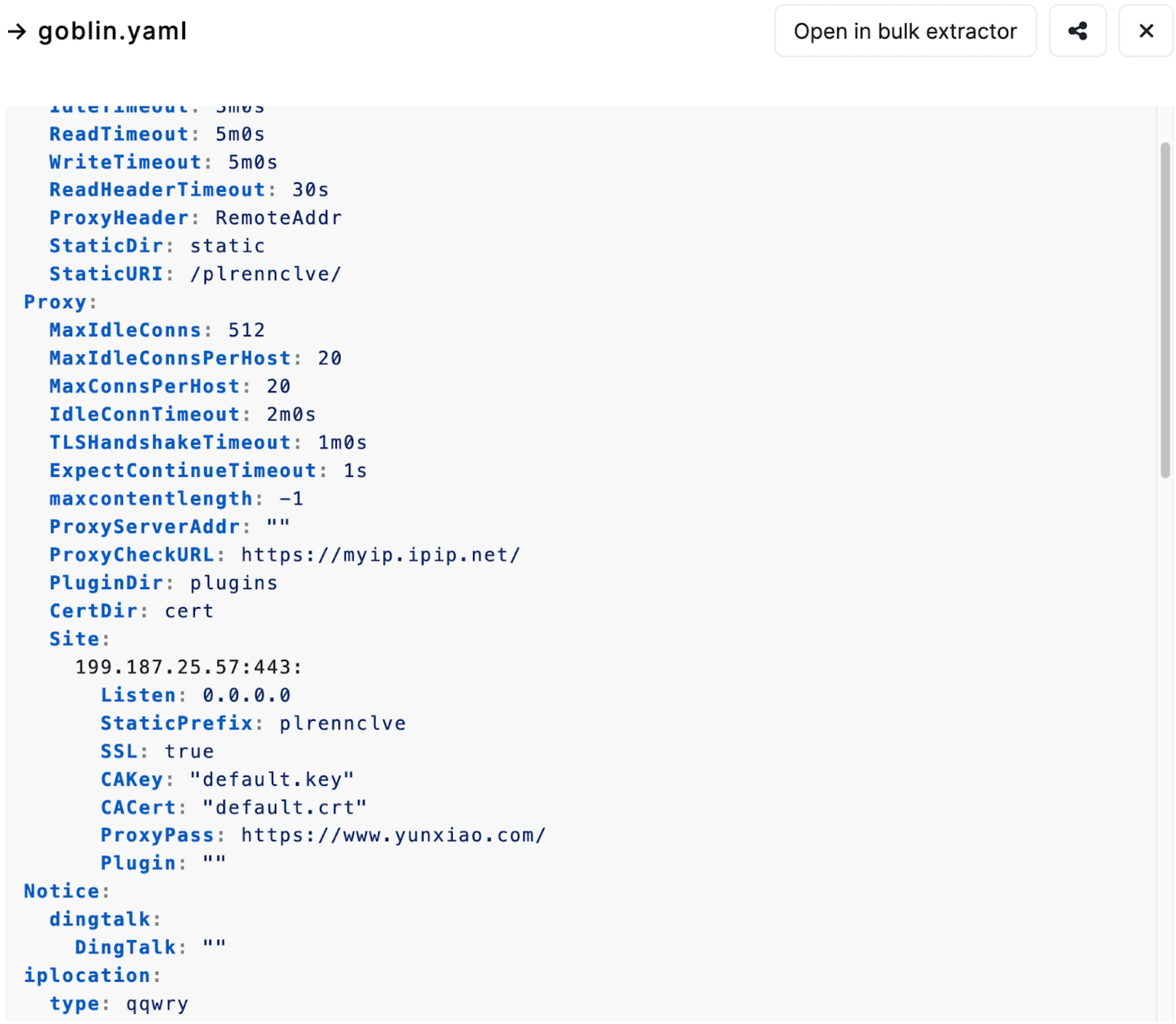
📒 中文 README | 📌 Releases Download | 📖 Documents

✴️ Features

- Support for caching static files to speed up access.
- Supports dumping all requests, dumping requests that match the rules.
- Support quick configuration through plug-ins to adjust inappropriate jumps or content.
- Support for implanting specific javacript code.
- Support for modifying the content of responses or goblin requests.
- Support hiding real IP by proxy.

Figure 4: Screenshot of the English-language README version of the Goblin Project (Source: GitHub)

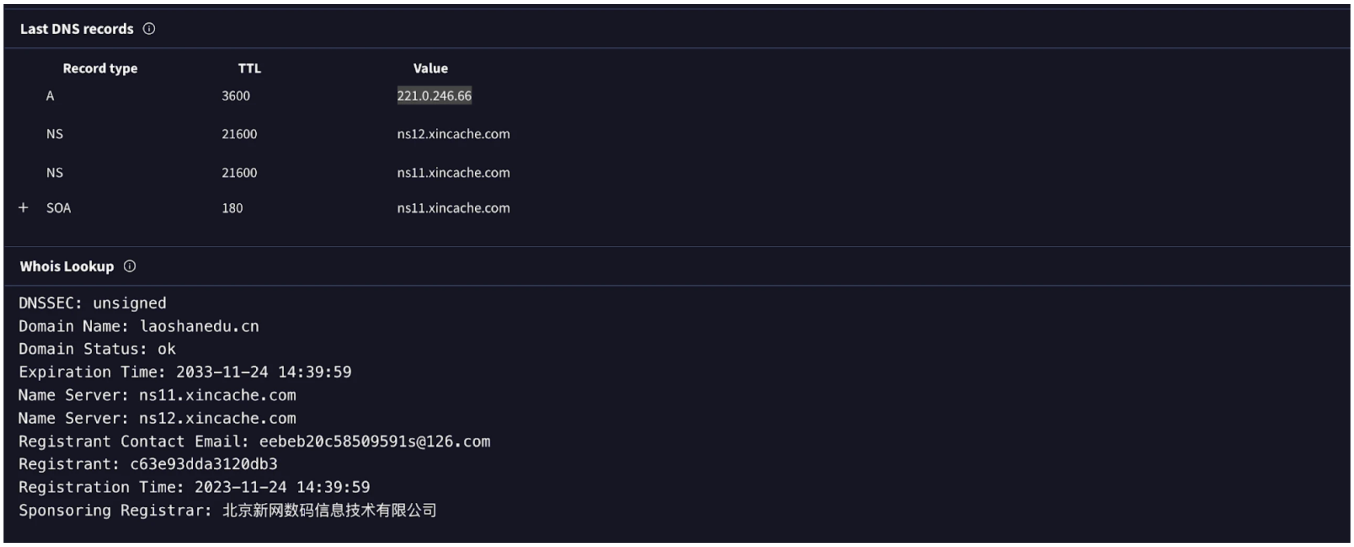
A review of Goblin's YAML configuration file in the directory reveals that the operator has configured traffic to proxy through yunxiao[.]com, a domain associated with Alibaba Cloud's Yunxiao DevOps platform, and laoshanedu.cn. While the purpose behind this setup remains unclear, our analysis failed to reveal any injected JavaScript or identifiable phishing targets.



```
  IdleTimeout: 5m0s
  ReadTimeout: 5m0s
  WriteTimeout: 5m0s
  ReadHeaderTimeout: 30s
  ProxyHeader: RemoteAddr
  StaticDir: static
  StaticURI: /plrennclve/
Proxy:
  MaxIdleConns: 512
  MaxIdleConnsPerHost: 20
  MaxConnsPerHost: 20
  IdleConnTimeout: 2m0s
  TLSHandshakeTimeout: 1m0s
  ExpectContinueTimeout: 1s
  maxcontentlength: -1
  ProxyServerAddr: ""
  ProxyCheckURL: https://myip.ipip.net/
  PluginDir: plugins
  CertDir: cert
  Site:
    199.187.25.57:443:
      Listen: 0.0.0.0
      StaticPrefix: plrennclve
      SSL: true
      CAKey: "default.key"
      CACert: "default.crt"
      ProxyPass: https://www.yunxiao.com/
      Plugin: ""
Notice:
  dingtalk:
    DingTalk: ""
iplocation:
  type: qqwry
```

Figure 5: Snippet of the Goblin YAML config file from the Hunt open directory page

Further analysis revealed that laoshanedu[.]cn was registered in November 2023 with Beijing Xinnet Digital Information Technology Co., Ltd. and used nameservers from xincache[.]com. Using an education-based naming format and recent setup suggests the domain may serve as a plausible cover for Goblin, potentially mimicking an educational institution.



Last DNS records ⓘ

	Record type	TTL	Value
	A	3600	221.0.246.66
	NS	21600	ns12.xincache.com
	NS	21600	ns11.xincache.com
+	SOA	180	ns11.xincache.com

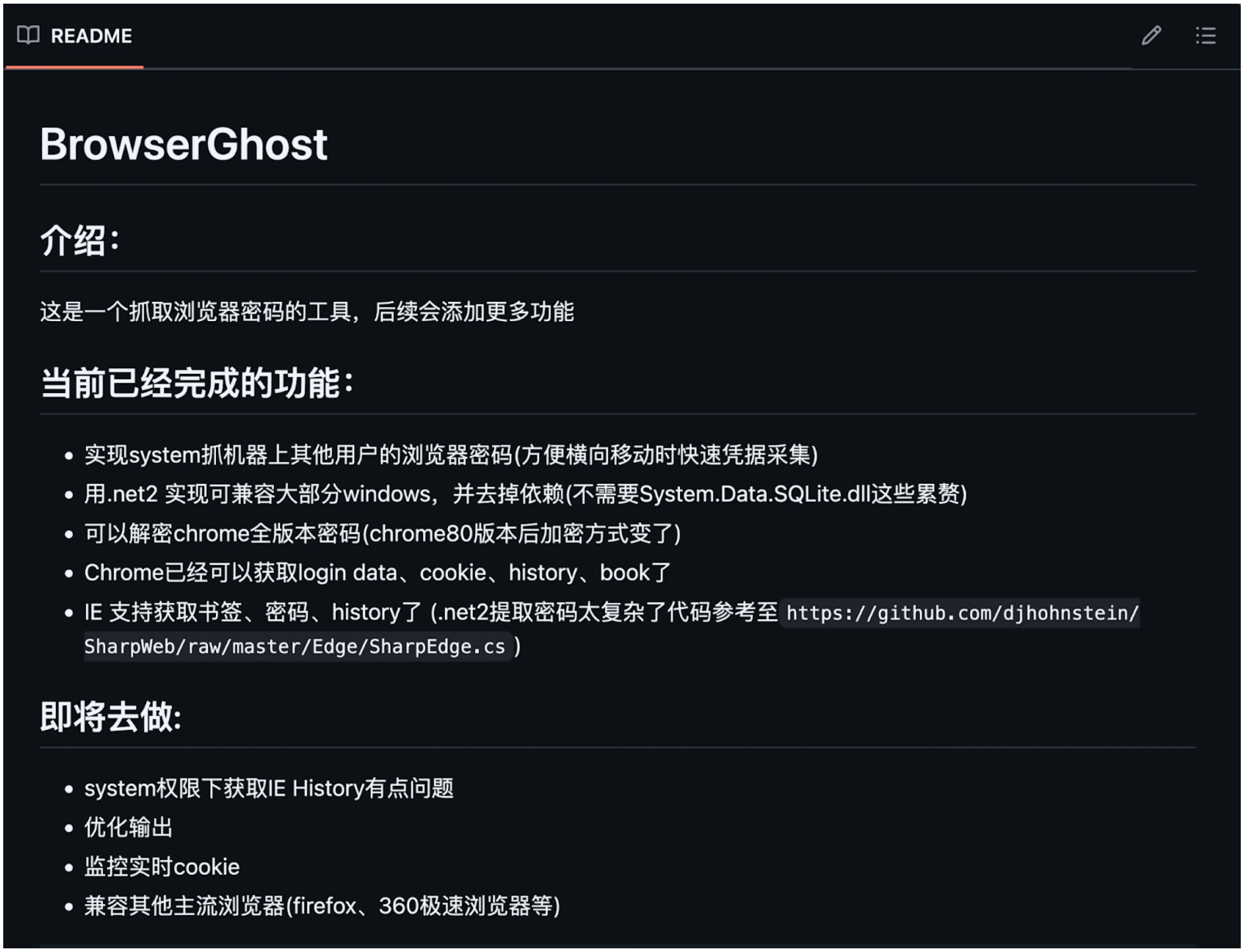
Whois Lookup ⓘ

```
DNSSEC: unsigned
Domain Name: laoshanedu.cn
Domain Status: ok
Expiration Time: 2033-11-24 14:39:59
Name Server: ns11.xincache.com
Name Server: ns12.xincache.com
Registrant Contact Email: eebeb20c58509591s@126.com
Registrant: c63e93dda3120db3
Registration Time: 2023-11-24 14:39:59
Sponsoring Registrar: 北京新网数码信息技术有限公司
```

Figure 6: DNS & WhoIs records in VirusTotal for laoshanedu[.]cn

BrowserGhost: A Phantom's Approach to Credential Access

The final tool we'll examine, BrowserGhost, is another open-source utility, this time found within the Cobalt Strike folder, designed to extract stored passwords from popular web browsers, including Chrome, Firefox, 360 Extreme, and Edge.



BrowserGhost

介绍:

这是一个抓取浏览器密码的工具，后续会添加更多功能

当前已经完成的功能:

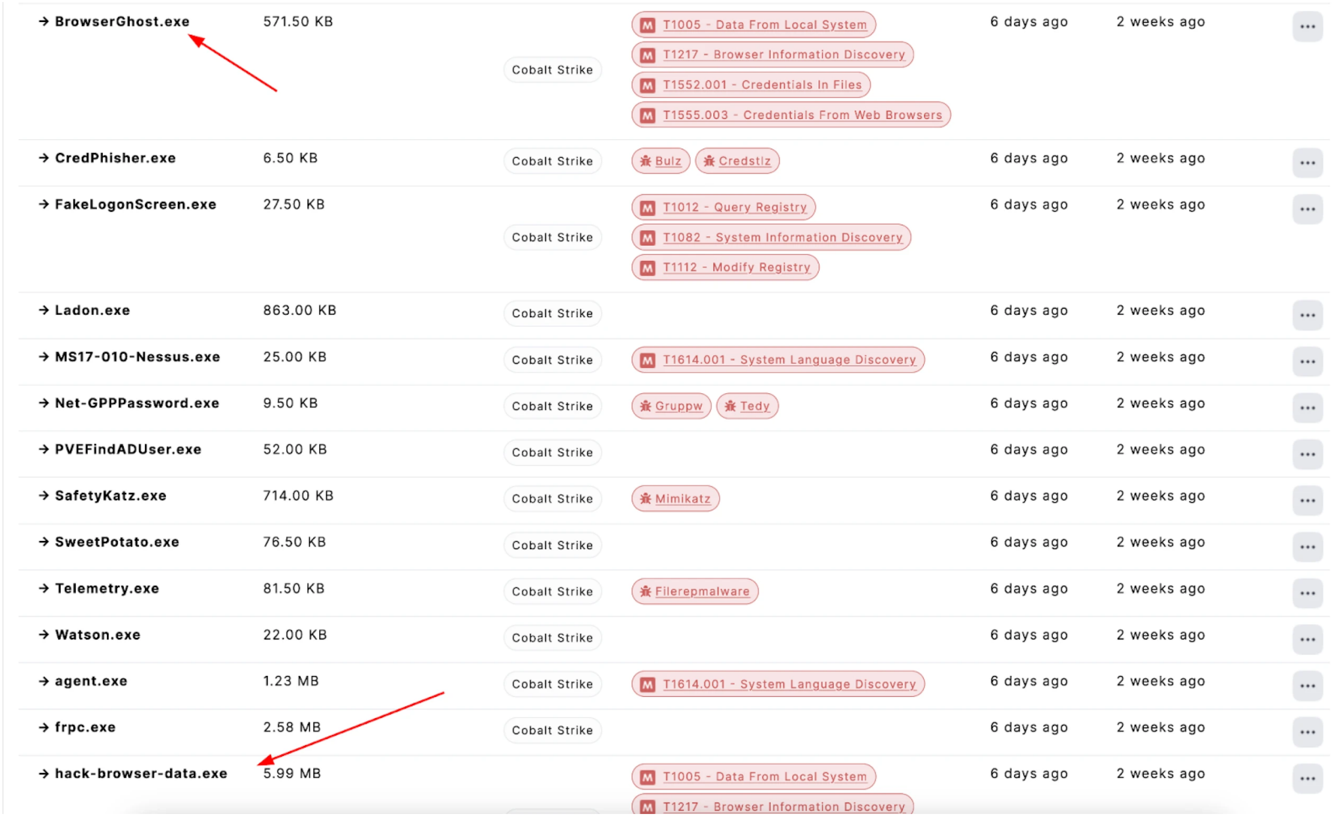
- 实现system抓机器上其他用户的浏览器密码(方便横向移动时快速凭据采集)
- 用.net2 实现可兼容大部分windows，并去掉依赖(不需要System.Data.SQLite.dll这些累赘)
- 可以解密chrome全版本密码(chrome80版本后加密方式变了)
- Chrome已经可以获取login data、cookie、history、book了
- IE 支持获取书签、密码、history了 (.net2提取密码太复杂了代码参考至 `https://github.com/djhohnstein/SharpWeb/raw/master/Edge/SharpEdge.cs`)

即将去做:

- system权限下获取IE History有点问题
- 优化输出
- 监控实时cookie
- 兼容其他主流浏览器(firefox、360极速浏览器等)

Figure 7: Screenshot of the BrowserGhost README in GitHub

Alongside BrowserGhost, the directory also contained HackBrowserData, a tool specifically built to extract and decrypt sensitive browser information. This combination of tools hints at an operator with a strong interest in harvesting browser-stored credentials, signaling a well-equipped red team or an adversary with a clear focus on data exfiltration from compromised systems.



→ BrowserGhost.exe	571.50 KB	Cobalt Strike	T1005 - Data From Local System T1217 - Browser Information Discovery T1552.001 - Credentials In Files T1555.003 - Credentials From Web Browsers	6 days ago	2 weeks ago	•••
→ CredPhisher.exe	6.50 KB	Cobalt Strike	Bulz Credstiz	6 days ago	2 weeks ago	•••
→ FakeLogonScreen.exe	27.50 KB	Cobalt Strike	T1012 - Query Registry T1082 - System Information Discovery T1112 - Modify Registry	6 days ago	2 weeks ago	•••
→ Ladon.exe	863.00 KB	Cobalt Strike		6 days ago	2 weeks ago	•••
→ MS17-010-Nessus.exe	25.00 KB	Cobalt Strike	T1614.001 - System Language Discovery	6 days ago	2 weeks ago	•••
→ Net-GPPPassword.exe	9.50 KB	Cobalt Strike	Gruppw Tedy	6 days ago	2 weeks ago	•••
→ PVEFindADUser.exe	52.00 KB	Cobalt Strike		6 days ago	2 weeks ago	•••
→ SafetyKatz.exe	714.00 KB	Cobalt Strike	Mimikatz	6 days ago	2 weeks ago	•••
→ SweetPotato.exe	76.50 KB	Cobalt Strike		6 days ago	2 weeks ago	•••
→ Telemetry.exe	81.50 KB	Cobalt Strike	Filerepmalware	6 days ago	2 weeks ago	•••
→ Watson.exe	22.00 KB	Cobalt Strike		6 days ago	2 weeks ago	•••
→ agent.exe	1.23 MB	Cobalt Strike	T1614.001 - System Language Discovery	6 days ago	2 weeks ago	•••
→ frpc.exe	2.58 MB	Cobalt Strike		6 days ago	2 weeks ago	•••
→ hack-browser-data.exe	5.99 MB		T1005 - Data From Local System T1217 - Browser Information Discovery	6 days ago	2 weeks ago	•••

Figure 8: Screenshot of multiple files within the cs4.2 folder, including BrowserGhost and HackBrowserData

Closing the Door on a Haunted Directory

In wrapping up our Halloween dive into this open directory, we've highlighted tools like Cobalt Strike, Goblin, and BrowserGhost—each with capabilities that extend from red teaming to potentially darker uses. Our findings highlight how such tools, although often seen in professional settings, can be used for more sinister purposes—a reminder of the treats and tricks still hidden within the cybersecurity threat landscape.

If you want to learn more about these spooky threats and light your Jack-o-lantern against their tricks, get in touch with Hunt.io!

Open Directory Observables

IP Address	Hosting Country	ASN	Cobalt Strike Watermark
1199.187.25[.]57:8899	HK	Cloudie Limited	1359593325

Shared Certificate (Major Cobalt Strike)

IP Address	Hosting Country	ASN	Domain(s)	Certificate
47.108.74[.]30	CN	Hangzhou Alibaba Advertising Co.,Ltd.	tbc.cbshscs.comtom[.]cn cbshscs.comtom[.]cn file.cbshscs.comtom[.]cn	Common Name: Major Cobalt Strike Country: Earth Org: cobaltstrike OrgUnit: AdvancedPenTesting City: Somewhere State: Cyberspace SHA-256 Hash: DFA9B3E8B5E0F229ECB2FB479544650D0B87EB8494CE176714CF4E53I

Cobalt Strike Watermark (1359593325) Overlaps

IP Address	Hosting Country	ASN	Domain(s)
43.134.183.43	HK	Tencent Building, Kejizhongyi Avenue	N/A
101.132.182.180	CN	Hangzhou Alibaba Advertising Co.,Ltd.	N/A

IP Address	Hosting Country	ASN	Domain(s)
106.15.40[.]123	CN	Hangzhou Alibaba Advertising Co.,Ltd.	N/A
39.98.196[.]145	CN	Zhejiang Taobao Network Co.,Ltd	N/A
94.74.105[.]131	HK	HUAWEI CLOUDS	N/A
1.15.247[.]249	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
1.117.72[.]154	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
27.102.118[.]70	SK	DAOU TECHNOLOGY	ns1.kjdfklha[.]top ns2.kjdfklha[.]top kjdfklha[.]top blog.kjdfklha[.]top
210.1.226.[.]164	MA	TechAvenue Malaysia	N/A
101.43.157[.]20	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
106.52.236[.]88	CN	Shenzhen Tencent Computer Systems Company Limited	src.idvfecx.qiniudns[.]com
111.231.140[.]197	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
124.221.167[.]192	CN	Shenzhen Tencent Computer Systems Company Limited	N/A
117.72.10[.]22	CN	Beijing Jingdong 360 Degree E-commerce Co., Ltd.	dn2ufncur4f3f[.]shop
119.3.153[.]81	CN	Huawei Cloud Service data center	N/A