Poison Ivy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:52:38 UTC

Poison Ivy

aka: SPIVY, pivy, poisonivy

Actor(s): GALLIUM, Molerats, Mustang Panda, Nightshade Panda, Pirate Panda, Stone Panda, TA428, Temper Panda

VTCollection

There is no description at this point.

References

2022-11-30 · · FFRI Security ·
Evolution of the PlugX loader
PlugX Poison Ivy

2022-08-22 · Fortinet · Fred Gutierrez, Shunichi Imano
A Tale of PivNoxy and Chinoxy Puppeteer
Chinoxy Poison Ivy

2022-07-31 · BushidoToken Blog · BushidoToken
Space Invaders: Cyber Threats That Are Out Of This World
Poison Ivy Raindrop SUNBURST TEARDROP WastedLocker

2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Crawling Taurus
Poison Ivy APT20

2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Shallow Taurus
FormerFirstRAT IsSpace NewCT PlugX Poison Ivy Tidepool DragonOK

2022-05-17 · Positive Technologies · Positive Technologies

Space Pirates: analyzing the tools and connections of a new hacker group

FormerFirstRAT PlugX Poison Ivy Rovnix ShadowPad Zupdax

2022-05-16 · JPCERT/CC · Shusei Tomonaga

Analysis of HUI Loader

HUI Loader PlugX Poison Ivy Quasar RAT

2021-06-16 · Recorded Future · Insikt Group®

Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries

Icefog PcShare PlugX Poison Ivy QuickHeal DAGGER PANDA

2021-03-17 · Recorded Future · Insikt Group®

China-linked TA428 Continues to Target Russia and Mongolia IT Companies

PlugX Poison Ivy TA428

2021-02-01 · ESET Research · Ignacio Sanmillan, Matthieu Faou

Operation NightScout: Supply-chain attack targets online gaming in Asia

Ghost RAT NoxPlayer Poison Ivy Red Dev 17

2021-01-15 · Swisscom · Markus Neis

Cracking a Soft Cell is Harder Than You Think

Ghost RAT MimiKatz PlugX Poison Ivy Trochilus RAT

2021-01-08 · Youtube (Virus Bulletin) · Fumio Ozawa, Rintaro Koike, Shogo Hayashi

Operation LagTime IT: colourful Panda footprint

Cotx RAT nccTrojan Poison Ivy Tmanger TA428

2020-10-30 · YouTube (Kaspersky Tech) · Kris McConkey

Around the world in 80 days 4.2bn packets

Cobalt Strike Derusbi HyperBro Poison Ivy ShadowPad Winnti

2020-10-01 · US-CERT · US-CERT

Alert (AA20-275A): Potential for China Cyber Response to Heightened U.S.-China Tensions

CHINACHOPPER Cobalt Strike Empire Downloader MimiKatz Poison Ivy

2020-09-30 · NTT Security · Fumio Ozawa, Rintaro Koike, Shogo Hayashi

Operation LagTime IT: colourful Panda footprint (Slides)

Cotx RAT nccTrojan Poison Ivy Tmanger

2020-09-30 · NTT Security · Fumio Ozawa, Rintaro Koike, Shogo Hayashi

Operation LagTime IT: colourful Panda footprint

Cotx RAT nccTrojan Poison Ivy Tmanger

2020-09-16 · RiskIQ · Jon Gross
RiskIQ: Adventures in Cookie Land - Part 2
8.t Dropper Chinoxy Poison Ivy

2020-08-28 · NTT · Fumio Ozawa, Rintaro Koike, Shogo Hayashi
Operation Lagtime IT: Colourful Panda Footprint
Cotx RAT Poison Ivy TA428

2020-08-19 · NTT Security · Fumio Ozawa, Rintaro Koike, Shogo Hayashi
Operation LagTime IT: Colorful Panda Footprint
8.t Dropper Cotx RAT Poison Ivy TA428

2020-03-12 · Check Point · Check Point Research
Vicious Panda: The COVID Campaign
8.t Dropper BYEBY Enfal Korlia Poison Ivy

2020-03-02 · Virus Bulletin · Alex Hinchliffe
Pulling the PKPLUG: the adversary playbook for the long-standing espionage activity of a Chinese nation-state adversary
HenBox Farseer PlugX Poison Ivy

2020-01-29 · nao_sec blog · nao_sec
An Overhead View of the Royal Road
BLACKCOFFEE Cotx RAT Datper DDKONG Derusbi Icefog Korlia NewCore RAT PLAINTEE Poison Ivy Sisfader

2020-01-09 · Lab52 · Jagaimo Kawaii
TA428 Group abusing recent conflict between Iran and USA
Poison Ivy

2020-01-01 · Secureworks · SecureWorks
BRONZE UNION
9002 RAT CHINACHOPPER Enfal Ghost RAT HttpBrowser HyperBro owaauth PlugX Poison Ivy ZXShell APT27

2020-01-01 · Secureworks · SecureWorks
BRONZE RIVERSIDE
Anel ChChes Cobalt Strike PlugX Poison Ivy Quasar RAT RedLeaves APT10

2020-01-01 · Secureworks · SecureWorks
BRONZE KEYSTONE
9002 RAT BLACKCOFFEE DeputyDog Derusbi HiKit PlugX Poison Ivy ZXShell APT17

2020-01-01 · Secureworks · SecureWorks
BRONZE FIRESTONE
9002 RAT Derusbi Empire Downloader PlugX Poison Ivy APT19

2020-01-01 · Secureworks · SecureWorks
ALUMINUM SARATOGA
BlackShades DarkComet Xtreme RAT Poison Ivy Quasar RAT Molerats

2019-12-12 · Microsoft · Microsoft Threat Intelligence Center
GALLIUM: Targeting global telecom
CHINACHOPPER Ghost RAT HTran MimiKatz Poison Ivy GALLIUM

2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser
Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions
MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell

2019-11-06 · VirusBulletin · Bowen Pan, Lion Gu
A vine climbing over the Great Firewall: a long-term attack against China
Poison Ivy ZXShell GreenSpot

2019-07-23 · Proofpoint · Dennis Schwarz, Michael Raggi, Proofpoint Threat Insight Team
Chinese APT “Operation LagTime IT” Targets Government Information Technology Agencies in Eastern Asia
8.t Dropper Cotx RAT Poison Ivy TA428

2019-06-25 · Cybereason · Cybereason Nocturnus
OPERATION SOFT CELL: A WORLDWIDE CAMPAIGN AGAINST TELECOMMUNICATIONS PROVIDERS
CHINACHOPPER HTran MimiKatz Poison Ivy Operation Soft Cell

2019-01-01 · Virus Bulletin · Bowen Pan, Lion Gu
A vine climbing over the Great Firewall: A long-term attack against China
Poison Ivy ZXShell

2018-09-21 · Qihoo 360 Technology · Qihoo 360
Poison Ivy Group and the Cyberespionage Campaign Against Chinese Military and Goverment
Poison Ivy

2018-05-15 · BSides Detroit · Keven Murphy, Stefano Maccaglia
IR in Heterogeneous Environment
Korlia Poison Ivy

2017-09-15 · Fortinet · Xiaopeng Zhang
Deep Analysis of New Poison Ivy/PlugX Variant - Part II
Poison Ivy

2017-08-31 · NCC Group · Ahmed Zaki
Analysing a recent Poison Ivy sample
Poison Ivy

2017-08-23 · Fortinet · Xiaopeng Zhang
Deep Analysis of New Poison Ivy Variant
Poison Ivy

2017-05-31 · MITRE · MITRE ATT&CK
PittyTiger
Enfal Ghost RAT MimiKatz Poison Ivy APT24

2016-11-22 · Palo Alto Networks Unit 42 · Jen Miller-Osborn, Robert Falcone, Tom Lancaster, Vicky Ray
Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy
Poison Ivy

2016-04-26 · Github (CyberMonitor) · Jason Jones
New Poison Ivy Activity Targeting Myanmar, Asian Countries
Poison Ivy

2016-04-22 · Palo Alto Networks Unit 42 · Brandon Levene, Jen Miller-Osborn, Micah Yates, Mike Scott
New Poison Ivy RAT Variant Targets Hong Kong Pro-Democracy Activists
Poison Ivy

2015-02-06 · CrowdStrike · CrowdStrike
CrowdStrike Global Threat Intel Report 2014
BlackPOS CryptoLocker Derusbi Elise Enfal EvilGrab Gameover P2P HttpBrowser MedusaHTTP Mirage Naikon NetTraveler pirpi PlugX Poison Ivy Sakula RAT Sinowal sykipot taidoor

2014-09-19 · Palo Alto Networks Unit 42 · Jen Miller-Osborn, Ryan Olson
Recent Watering Hole Attacks Attributed to APT Group “th3bug” Using Poison Ivy
Poison Ivy

2014-01-01 · FireEye · FireEye
Operation Quantum Entanglement
IsSpace NewCT Poison Ivy SysGet

2013-10-31 · FireEye · Ned Moran, Thoufique Haq
Know Your Enemy: Tracking A Rapidly Evolving APT Actor
Bozok Poison Ivy TEMPER PANDA

2013-08-23 · FireEye · Nart Villeneuve, Ned Moran, Thoufique Haq
Operation Molerats: Middle East Cyber Attacks Using Poison Ivy
Poison Ivy Molerats

2011-01-01 · Symantec · Erica Eng, Gavin O'Gorman
The Nitro Attacks: Stealing Secrets from the Chemical Industry
Poison Ivy Nitro

2010-01-01 · Mandiant · Ero Carrera, Peter Silberman
State of Malware: Family Ties

Bredolab Conficker Cutwail KoobFace Oderoor Poison Ivy Rustock Sinowal Szribi Zeus

Yara Rules

▶ [TLP:WHITE] win_poison_ivy_auto (20251219 | Detects win.poison_ivy.)	
▶ [TLP:WHITE] win_poison_ivy_w0 (20170517 | No description)	

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_ivy