ShadowPad (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:05:04 UTC

There is no description at this point.

2026-01-20 · · Rostelecom-Solar ·
ShadowRelay – a unique backdoor in the public sector
ShadowPad SNAPPYBEE 2025-10-22 · Trend Micro · Daniel Lunghi, Joseph C Chen, Lenart Bermejo, Leon M Chang, Vickie Su
The Rise of Collaborative Tactics Among China-aligned Cyber Espionage Campaigns
Cobalt Strike DracuLoader ShadowPad 2025-06-09 · Sentinel LABS · Aleksandar Milenkoski, Tom Hegel
Follow the Smoke | China-nexus Threat Actors Hammer At the Doors of Top Tier Targets
GOREshell Nimbo-C2 ShadowPad 2025-04-08 · Hunt.io · Hunt.io
State-Sponsored Tactics: How Gamaredon and ShadowPad Operate and Rotate Their Infrastructure
ShadowPad 2025-03-20 · ESET Research · Matthieu Faou
Operation FishMedley
ShadowPad SodaMaster Spyder Earth Lusca FishMedley 2025-02-20 · Trend Micro · Daniel Lunghi
Updated Shadowpad Malware Leads to Ransomware Deployment
EvilExtractor PlugX ShadowPad Teleboyi 2025-02-20 · Trend Micro · Daniel Lunghi
Updated Shadowpad Malware Leads to Ransomware Deployment
EvilExtractor NailaoLocker PlugX ShadowPad 2025-02-20 · Orange Cyberdefense · Alexis Bonnefoi, Marine PICHON
Meet NailaoLocker: a ransomware distributed in Europe by ShadowPad and PlugX backdoors
NailaoLocker PlugX ShadowPad 2025-02-18 · Orange Cyberdefense · Alexis Bonnefoi, Marine PICHON
IOCs Green Nailao campaign (NailaoLocker, ShadowPad)
NailaoLocker PlugX ShadowPad 2025-01-29 · Google · Conor Quigley, Luke Jenkins, Nino Isakovic
ScatterBrain: Unmasking the Shadow of PoisonPlug's Obfuscator
POISONPLUG ShadowPad SNAPPYBEE 2025-01-21 · Trend Micro · Leon Chang, Theo Chen
Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions
Cobalt Strike HemiGate ShadowPad SNAPPYBEE SparrowDoor UNC4841 2024-08-01 · Cisco · Ashley Shen, Joey Chen, Vitor Ventura
APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike
Cobalt Strike ShadowPad 2024-05-23 · ITOCHU · ITOCHU Cyber & Intelligence Inc.
Malware Transmutation! - Unveiling the Hidden Traces of BloodAlchemy
BloodAlchemy ShadowPad 2024-03-18 · Trend Micro · Daniel Lunghi, Joseph C Chen
Earth Krahang Exploits Intergovernmental Trust to Launch Cross-Government Attacks
DinodasRAT PlugX Reshell ShadowPad Earth Krahang 2024-03-05 · Reliaquest · RELIAQUEST THREAT RESEARCH TEAM
Anxun and Chinese APT Activity
ShadowPad 2024-03-01 · HarfangLab · HarfangLab CTR
A Comprehensive Analysis of i-SOON’s Commercial Offering

ShadowPad Winnti 2024-02-21 · YouTube (SentinelOne) · Kris McConkey

LABSCon23 Replay | Chasing Shadows | The rise of a prolific espionage actor

9002 RAT PlugX ShadowPad Spyder Earth Lusca 2024-02-09 · Hunt.io · Michael R

Tracking ShadowPad Infrastructure Via Non-Standard Certificates

ShadowPad 2024-01-09 · Recorded Future · Insikt Group

2023 Adversary Infrastructure Report

AsyncRAT Cobalt Strike Emotet PlugX ShadowPad 2023-11-07 · Youtube (Virus Bulletin) · Daniel Lunghi

Possible supply chain attack targeting South Asian government delivers Shadowpad

ShadowPad 2023-10-04 · Trend Micro · Daniel Lunghi

Possible supply chain attack targeting Pakistan government delivers ShadowPad

ShadowPad 2023-10-04 · Trend Micro · Daniel Lunghi

Possible supply chain attack targeting Pakistan government delivers Shadowpad (Slides)

ShadowPad 2023-09-22 · Palo Alto Networks Unit 42 · Lior Rochberger, Robert Falcone, Tom Fakterman

Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda

Cobalt Strike MimiKatz RemCom ShadowPad TONESHELL 2023-09-12 · Symantec · Threat Hunter Team

Redfly: Espionage Actors Continue to Target Critical Infrastructure

ShadowPad Redfly 2023-08-07 · Recorded Future · Insikt Group

RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale

Winnti Brute Ratel C4 Cobalt Strike FunnySwitch PlugX ShadowPad Spyder Earth Lusca 2023-07-14 · Trend Micro · Daniel Lunghi

Possible Supply-Chain Attack Targeting Pakistani Government Delivers Shadowpad

ShadowPad DriftingCloud Tonto Team 2023-05-15 · Symantec · Threat Hunter Team

Lancefly: Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors

Merdoor PlugX ShadowPad ZXShell Lancefly 2023-02-02 · Elastic · Andrew Pease, Cyril François, Devon Kerr, Remco Sprooten, Salim Bitam, Seth Goodwin

Update to the REF2924 intrusion set and related campaigns

DoorMe ShadowPad SiestaGraph 2023-01-14 · YouTube (CODE BLUE) · Takahiro Haruyama

[CB22]Tracking the Entire Iceberg - Long-term APT Malware C2 Protocol Emulation and Scanning

ShadowPad Winnti 2022-10-27 · vmware · Takahiro Haruyama

Threat Analysis: Active C2 Discovery Using Protocol Emulation Part3 (ShadowPad)

ShadowPad 2022-10-25 · VMware Threat Analysis Unit · Takahiro Haruyama

Tracking the entire iceberg: long-term APT malware C2 protocol emulation and scanning

ShadowPad Winnti 2022-09-30 · NCC Group · Michael Mullen, Nikolaos Pantazopoulos, William Backhouse

A glimpse into the shadowy realm of a Chinese APT: detailed analysis of a ShadowPad intrusion

ShadowPad 2022-09-26 · Youtube (Virus Bulletin) · Takahiro Haruyama

Tracking the entire iceberg long term APT malware C2 protocol emulation and scanning

ShadowPad Winnti 2022-09-19 · Virus Bulletin · Takahiro Haruyama

Tracking the entire iceberg - long-term APT malware C2 protocol emulation and scanning

ShadowPad Winnti 2022-09-13 · Symantec · Threat Hunter Team

New Wave of Espionage Activity Targets Asian Governments

MimiKatz PlugX Quasar RAT ShadowPad Trochilus RAT 2022-09-06 · ESET Research · Thibaut Passilly

Worok: The big picture

MimiKatz PNGLoad reGeorg ShadowPad Worok 2022-07-01 · RiskIQ · RiskIQ

ToddyCat: A Guided Journey through the Attacker's Infrastructure

ShadowPad ToddyCat 2022-06-27 · Kaspersky ICS CERT · Artem Snegirev, Kirill Kruglov

Attacks on industrial control systems using ShadowPad

Cobalt Strike PlugX ShadowPad 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 2022-05-12 · TEAMT5 · Leon Chang, Silvia Yeh

The Next Gen PlugX/ShadowPad? A Dive into the Emerging China-Nexus Modular Trojan, Pangolin8RAT (slides)

KEYPLUG Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad Winnti SLIME29 TianWu 2022-05-02 · Sentinel LABS · Amitai Ben Shushan Ehrlich, Joey Chen

Moshen Dragon’s Triad-and-Error Approach | Abusing Security Software to Sideload PlugX and ShadowPad

PlugX ShadowPad Moshen Dragon 2022-04-08 · The Register · Laura Dobberstein

China accused of cyberattacks on Indian power grid

ShadowPad 2022-04-06 · Recorded Future · Insikt Group®

Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group (TAG-38)

ShadowPad 2022-04-06 · Recorded Future · Insikt Group

Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group

ShadowPad 2022-02-23 · Dragos · Dragos

2021 ICS OT Cybersecurity Year In Review

ShadowPad 2022-02-15 · The Hacker News · Ravie Lakshmanan

Researchers Link ShadowPad Malware Attacks to Chinese Ministry and PLA

ShadowPad 2022-02-15 · Secureworks · Counter Threat Unit ResearchTeam

ShadowPad Malware Analysis

ShadowPad 2022-01-17 · Trend Micro · Cedric Pernet, Daniel Lunghi, Gloria Chen, Jaromír Hořejší, Joseph Chen, Kenney Lu

Delving Deep: An Analysis of Earth Lusca’s Operations

BIOPASS Cobalt Strike FunnySwitch JuicyPotato ShadowPad Winnti Earth Lusca 2021-12-17 · FBI · FBI

AC-000159-MW: APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop Central (CVE-2021-44515)

ShadowPad 2021-12-16 · TEAMT5 · Aragorn Tseng, Charles Li, Peter Syu, Tom Lai

Winnti is Coming - Evolution after Prosecution

Cobalt Strike FishMaster FunnySwitch HIGHNOON ShadowPad Spyder 2021-12-08 · PWC UK · Adam Prescott

Chasing Shadows: A deep dive into the latest obfuscation methods being used by ShadowPad

ShadowPad Earth Lusca 2021-11-19 · insomniacs(Medium) · Asuna Amawaka

It’s a BEE! It’s a… no, it’s ShadowPad.

ShadowPad 2021-11-04 · Youtube (Virus Bulletin) · Joey Chen, Yi-Jhen Hsieh

ShadowPad: the masterpiece of privately sold malware in Chinese espionage

PlugX ShadowPad 2021-10-26 · Kaspersky · Kaspersky Lab ICS CERT

APT attacks on industrial organizations in H1 2021

8.t Dropper AllaKore AsyncRAT GoldMax LimeRAT NjRAT NoxPlayer Raindrop ReverseRAT ShadowPad Zebrocy 2021-09-01 · YouTube (Hack In The Box Security Conference) · Joey Chen, Yi-Jhen Hsieh

SHADOWPAD: Chinese Espionage Malware-as-a-Service

PlugX ShadowPad 2021-08-23 · SentinelOne · Joey Chen, Yi-Jhen Hsieh

ShadowPad: the Masterpiece of Privately Sold Malware in Chinese Espionage

PlugX ShadowPad 2021-08-19 · Sentinel LABS · Joey Chen, Yi-Jhen Hsieh

ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage

ShadowPad 2021-08-12 · Sentinel LABS · SentinelLabs

ShadowPad: A Masterpiece of Privately Sold Malware in Chinese Espionage

ShadowPad Earth Lusca 2021-07-08 · Recorded Future · Insikt Group®

Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling

ShadowPad Spyder Winnti 2021-07-08 · · PTSecurity · Denis Kuvshinov

How winnti APT grouping works

Korlia ShadowPad Winnti 2021-07-08 · · YouTube (PT Product Update) · Denis Kuvshinov

How winnti APT grouping works

Korlia ShadowPad Winnti 2021-04-29 · NTT · Threat Detection NTT Ltd.

The Operations of Winnti group

Cobalt Strike ShadowPad Spyder Winnti Earth Lusca 2021-03-29 · The Record · Catalin Cimpanu

RedEcho group parks domains after public exposure

PlugX ShadowPad RedEcho 2021-02-28 · Recorded Future · Insikt Group®

China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

PlugX ShadowPad RedEcho 2021-02-28 · Recorded Future · Insikt Group®

China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions

Icefog PlugX ShadowPad 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 2021-01-14 · PTSecurity · PT ESC Threat Intelligence

Higaisa or Winnti? APT41 backdoors, old and new

Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad 2020-12-10 · ESET Research · Mathieu Tartare

Operation StealthyTrident: corporate software under attack

HyperBro PlugX ShadowPad Tmanger 2020-11-23 · Youtube (OWASP DevSlop) · Negar Shabab, Noushin Shabab

Compromised Compilers - A new perspective of supply chain cyber attacks

ShadowPad 2020-11-03 · Kaspersky Labs · GReAT

APT trends report Q3 2020

WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti 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 2020-10-27 · Dr.Web · Dr.Web

Study of the ShadowPad APT backdoor and its relation to PlugX

Ghost RAT PlugX ShadowPad 2020-09-18 · Symantec · Threat Hunter Team

APT41: Indictments Put Chinese Espionage Group in the Spotlight

CROSSWALK PlugX POISONPLUG ShadowPad Winnti 2020-09-08 · PTSecurity · PTSecurity

ShadowPad: new activity from the Winnti group

CCleaner Backdoor Korlia ShadowPad TypeHash 2020-07-29 · Kaspersky Labs · GReAT

APT trends report Q2 2020

PhantomLance Dacls Penquin Turla elf.wellmess AppleJeus Dacls AcidBox Cobalt Strike Dacls EternalPetya Godlike12 Olympic Destroyer PlugX shadowhammer ShadowPad Sinowal VHD Ransomware Volgmer WellMess X-Agent XTunnel 2020-07-14 · CrowdStrike · Falcon OverWatch Team

Manufacturing Industry in the Adversaries' Crosshairs

ShadowPad Snake 2020-06-25 · Dr.Web · Dr.Web

BackDoor.ShadowPad.1

ShadowPad 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-01-31 · ESET Research · Mathieu Tartare

Winnti Group targeting universities in Hong Kong

ShadowPad Winnti 2019-10-07 · ESET Research · Marc-Etienne M.Léveillé, Mathieu Tartare

CONNECTING THE DOTS: Exposing the arsenal and methods of the Winnti Group

LOWKEY shadowhammer ShadowPad 2019-09-23 · MITRE · MITRE ATT&CK

APT41

Derusbi MESSAGETAP Winnti ASPXSpy BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT MimiKatz NjRAT PlugX ShadowPad Winnti ZXShell APT41 2019-04-23 · Kaspersky Labs · AMR, GReAT

Operation ShadowHammer: a high-profile supply chain attack

shadowhammer ShadowPad 2019-04-22 · Trend Micro · Mohamad Mokbel

C/C++ Runtime Library Code Tampering in Supply Chain

shadowhammer ShadowPad Winnti 2017-08-15 · Kaspersky Labs · GReAT

ShadowPad in corporate networks

ShadowPad

▶ [TLP:WHITE] win_shadowpad_auto (20251219 | Detects win.shadowpad.)
