PlugX (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:25:30 UTC

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

Notable features of this malware family are the ability to execute commands on the affected machine to retrieve:
machine information
capture the screen
send keyboard and mouse events
keylogging
reboot the system
manage processes (create, kill and enumerate)
manage services (create, start, stop, etc.); and
manage Windows registry entries, open a shell, etc.

The malware also logs its events in a text log file.

2026-02-26 · Lab52 ·
PlugX Meeting Invitation via MSBuild and GDATA
PlugX 2025-10-30 · Arctic Wolf · Arctic Wolf Labs Team
UNC6384 Weaponizes ZDI-CAN-25373 Vulnerability to Deploy PlugX Against Hungarian and Belgian Diplomatic Entities
PlugX 2025-08-25 · Google · Google Threat Intelligence Group
Deception in Depth: PRC-Nexus Espionage Campaign Hijacks Web Traffic to Target Diplomats
PlugX UNC6384 2025-03-14 · bluecyber · Ngo Thanh Van
PlugX: Bad guy disguises as an msi file
PlugX 2025-02-20 · Orange Cyberdefense · Alexis Bonnefoi, Marine PICHON
Meet NailaoLocker: a ransomware distributed in Europe by ShadowPad and PlugX backdoors
NailaoLocker PlugX ShadowPad 2025-02-20 · Trend Micro · Daniel Lunghi
Updated Shadowpad Malware Leads to Ransomware Deployment
EvilExtractor NailaoLocker PlugX ShadowPad 2025-02-20 · Trend Micro · Daniel Lunghi
Updated Shadowpad Malware Leads to Ransomware Deployment
EvilExtractor PlugX ShadowPad Teleboyi 2025-02-18 · Orange Cyberdefense · Alexis Bonnefoi, Marine PICHON
IOCs Green Nailao campaign (NailaoLocker, ShadowPad)
NailaoLocker PlugX ShadowPad 2025-02-13 · Symantec · Threat Hunter Team
China-linked Espionage Tools Used in Ransomware Attacks
PlugX 2025-01-29 · Palo Alto Networks Unit 42 · Lior Rochberger, Yoav Zemah

CL-STA-0048: An Espionage Operation Against High-Value Targets in South Asia
Cobalt Strike MimiKatz PlugX ValleyRAT Winos CL-STA-0048 2025-01-14 · Department of Justice · Office of Public Affairs
Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers
PlugX 2025-01-09 · Recorded Future · Insikt Group
Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain
PlugX 2024-10-10 · Hunt.io · Hunt.io
Unmasking Adversary Infrastructure: How Certificates and Redirects Exposed Earth Baxia and PlugX Activity
Cobalt Strike PlugX 2024-09-24 · Virus Bulletin · Aragorn Tseng, Chi-Yu You, Cristiana Brafman Kittner, Steve Su
Down the GRAYRABBIT HOle - Exposing UNC3569 and its Modus Operandi
KEYPLUG Cobalt Strike CROSSWALK GRAYRABBIT HelloBot HUI Loader PlugX SiestaGraph 2024-09-10 · Talos Intelligence · Joey Chen
DragonRank, a Chinese-speaking SEO manipulator service provider
IISpy PlugX DragonRank 2024-08-23 · TEAMT5 · Still Hsu
Sailing the Seven SEAs: Deep Dive into Polaris' Arsenal and Intelligence Insights
Cobalt Strike Hodur PlugX TONESHELL 2024-06-03 · SYGNIA · Sygnia Team
China-Nexus Threat Group ‘Velvet Ant’ Abuses F5 Load Balancers for Persistence
PlugX 2024-05-23 · Palo Alto Networks Unit 42 · Daniel Frank, Lior Rochberger
Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia
Agent Racoon CHINACHOPPER Ghost RAT JuicyPotato MimiKatz Ntospy PlugX SweetSpecter TunnelSpecter CL-STA-0043 2024-04-27 · Google · Rommel-J
Finding Malware: Detecting SOGU with Google Security Operations.
PlugX 2024-04-19 · · Spiegel Online · Christoph Giesen, Hakan Tanriverdi, Simon Hage
VW-Konzern wurde jahrelang ausspioniert – von China?
CHINACHOPPER PlugX 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 2024-02-21 · YouTube (SentinelOne) · Kris McConkey
LABSCon23 Replay | Chasing Shadows | The rise of a prolific espionage actor
9002 RAT PlugX ShadowPad Spyder Earth Lusca 2024-01-25 · JSAC 2024 · Yi-Chin Chuang, Yu-Tung Chang
Unveiling TeleBoyi: Chinese APT Group Targeting Critical Infrastructure Worldwide
PlugX 2024-01-25 · JSAC 2024 · Hara Hiroaki, Kawakami Ryonosuke, Shota Nakajima
The Secret Life of RATs: connecting the dots by dissecting multiple backdoors
DracuLoader GroundPeony HemiGate PlugX 2024-01-23 · CSIRT-CTI · CSIRT-CTI
Stately Taurus Targets Myanmar Amidst Concerns over Military Junta’s Handling of Rebel Attacks
PlugX PUBLOAD TONESHELL 2024-01-21 · Mahmoud Zohdy Blog · Mahmoud Zohdy
A Look into PlugX Kernel driver
PlugX 2024-01-09 · Recorded Future · Insikt Group
2023 Adversary Infrastructure Report
AsyncRAT Cobalt Strike Emotet PlugX ShadowPad 2023-12-06 · splunk · Splunk Threat Research Team
Unmasking the Enigma: A Historical Dive into the World of PlugX Malware

PlugX 2023-12-06 · MITRE · MITRE ATT&CK

Cinnamon Tempest

Cobalt Strike HUI Loader PlugX Sliver BRONZE STARLIGHT 2023-09-08 · PolySwarm Tech Team · The Hivemind

Carderbee Targets Hong Kong in Supply Chain Attack

PlugX Carderbee 2023-09-07 · Sekoia · Jamila B.

My Tea's not cold. An overview of China's cyber threat

Melofee PingPull SoWaT Sword2033 MgBot MQsTTang PlugX TONESHELL Dalbit MirrorFace 2023-08-22 · Symantec · Threat Hunter Team

Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong

PlugX Carderbee 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 2023-07-11 · Mandiant · Ng Choon Kiat, Rommel Joven

The Spies Who Loved You: Infected USB Drives to Steal Secrets

PlugX 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 2023-05-03 · Lab52 · Lab52

New Mustang Panda's campaing against Australia

PlugX 2023-04-23 · ESET Research · Alexandre Côté Cyr, Matthieu Faou

TA410: APT10's distant cousin

FlowCloud Lookback PlugX Quasar RAT Tendyron Witchetty 2023-04-18 · Mandiant · Mandiant

M-Trends 2023

QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate 2023-03-30 · Recorded Future · Insikt Group

With KEYPLUG, China's RedGolf Spies On, Steals From Wide Field of Targets

KEYPLUG Cobalt Strike PlugX RedGolf 2023-03-09 · ASEC · Sanseo

PlugX Malware Being Distributed via Vulnerability Exploitation

PlugX 2023-03-09 · Sophos · Gabor Szappanos

A border-hopping PlugX USB worm takes its act on the road

PlugX 2023-02-24 · Trend Micro · Buddy Tancio, Catherine Loveria, Jed Valderama

Investigating the PlugX Trojan Disguised as a Legitimate Windows Debugger Tool

PlugX 2023-02-02 · EclecticIQ · EclecticIQ Threat Research Team

Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware

PlugX 2023-01-26 · Palo Alto Networks Unit 42 · Jen Miller-Osborn, Mike Harbison

Chinese PlugX Malware Hidden in Your USB Devices?

PlugX 2023-01-26 · TEAMT5 · Still Hsu

Brief History of MustangPanda and its PlugX Evolution

PlugX MUSTANG PANDA 2023-01-09 · kienmanowar Blog · m4n0w4r, Tran Trung Kien

[QuickNote] Another nice PlugX sample

PlugX 2022-12-27 · kienmanowar Blog · m4n0w4r, Tran Trung Kien

Diving into a PlugX sample of Mustang Panda group

PlugX 2022-12-06 · Blackberry · BlackBerry Research & Intelligence Team

Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets

PlugX 2022-12-02 · Avast Decoded · Threat Intelligence Team

Hitching a ride with Mustang Panda

PlugX 2022-11-30 · · FFRI Security · Matsumoto

Evolution of the PlugX loader

PlugX Poison Ivy 2022-10-06 · Blackberry · The BlackBerry Research & Intelligence Team

Mustang Panda Abuses Legitimate Apps to Target Myanmar Based Victims

PlugX 2022-09-26 · Palo Alto Networks Unit 42 · Daniela Shalev, Itay Gamliel

Hunting for Unsigned DLLs to Find APTs

PlugX Raspberry Robin Roshtyak 2022-09-14 · Security Joes · Felipe Duarte

Dissecting PlugX to Extract Its Crown Jewels

PlugX 2022-09-13 · Symantec · Threat Hunter Team

New Wave of Espionage Activity Targets Asian Governments

MimiKatz PlugX Quasar RAT ShadowPad Trochilus RAT 2022-09-09 · Github (m4now4r) · m4n0w4r

“Mustang Panda” – Enemy at the gate

PlugX 2022-09-08 · Cybereason · Aleksandar Milenkoski, Kotaro Ogino, Yuki Shibuya

Threat Analysis Report: PlugX RAT Loader Evolution

PlugX 2022-09-08 · Secureworks · Counter Threat Unit ResearchTeam

BRONZE PRESIDENT Targets Government Officials

PlugX 2022-07-18 · YouTube (Security Joes) · Felipe Duarte

PlugX DLL Side-Loading Technique

PlugX 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Shallow Taurus

FormerFirstRAT IsSpace NewCT PlugX Poison Ivy Tidepool DragonOK 2022-06-27 · Kaspersky ICS CERT · Artem Snegirev, Kirill Kruglov

Attacks on industrial control systems using ShadowPad

Cobalt Strike PlugX ShadowPad 2022-06-23 · Secureworks · Counter Threat Unit ResearchTeam

BRONZE STARLIGHT Ransomware Operations Use HUI Loader

ATOMSILO Cobalt Strike HUI Loader LockFile NightSky Pandora PlugX Quasar RAT Rook SodaMaster

BRONZE STARLIGHT 2022-05-23 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

Operation Earth Berberoka

reptile oRAT Ghost RAT PlugX pupy Earth Berberoka 2022-05-20 · VinCSS · Dang Dinh Phuong, m4n0w4r, Tran Trung Kien

[RE027] China-based APT Mustang Panda might have still continued their attack activities against organizations in Vietnam

PlugX 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 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 2022-05-05 · Cisco Talos · Aliza Berk, Asheer Malhotra, Jung soo An, Justin Thattil, Kendall McKay

Mustang Panda deploys a new wave of malware targeting Europe

Cobalt Strike Meterpreter PlugX PUBLOAD 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 2022-04-28 · PWC · PWC UK

Cyber Threats 2021: A Year in Retrospect (Annex)

Cobalt Strike Conti PlugX RokRAT Inception Framework Red Menshen 2022-04-28 · DARKReading · Jai Vijayan

Chinese APT Bronze President Mounts Spy Campaign on Russian Military

PlugX MUSTANG PANDA 2022-04-27 · Trendmicro · Daniel Lunghi, Jaromír Hořejší

Operation Gambling Puppet

reptile oRAT AsyncRAT Cobalt Strike DCRat Ghost RAT PlugX Quasar RAT Trochilus RAT Earth Berberoka 2022-04-27 · Trendmicro · Trendmicro

IOCs for Earth Berberoka - Windows

AsyncRAT Cobalt Strike PlugX Quasar RAT Earth Berberoka 2022-04-27 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware

HelloBot AsyncRAT Ghost RAT HelloBot PlugX Quasar RAT Earth Berberoka 2022-04-14 · NSHC RedAlert Labs · NSHC Threatrecon Team

Hacking activity of SectorB Group in 2021 Chinese government supported hacking group SectorB

PlugX 2022-04-12 · Max Kersten's Blog · Max Kersten

Ghidra script to handle stack strings

CaddyWiper PlugX 2022-03-28 · Trellix · Marc Elias, Max Kersten

PlugX: A Talisman to Behold

PlugX 2022-03-25 · · ESET Research · Alexandre Côté Cyr

Mustang Panda's Hodur: Old stuff, new variant of Korplug

PlugX 2022-03-24 · Threat Post · Nate Nelson

Chinese APT Combines Fresh Hodur RAT with Complex Anti-Detection

PlugX 2022-03-23 · ESET Research · Alexandre Côté Cyr

Mustang Panda’s Hodur: Old tricks, new Korplug variant

Hodur PlugX 2022-03-23 · BleepingComputer · Bill Toulas

New Mustang Panda hacking campaign targets diplomats, ISPs

PlugX 2022-03-07 · Proofpoint · Michael Raggi, Myrtus 0x0

The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates

PlugX MUSTANG PANDA 2022-02-17 · SinaCyber · Adam Kozy

Testimony before the U.S.-China Economic and Security Review Commission Hearing on “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

PlugX APT26 APT41 2022-01-06 · Cyber And Ramen blog · Mike R

A “GULP” of PlugX

PlugX 2021-12-01 · ESET Research · Alexis Dorais-Joncas, Facundo Muñoz

Jumping the air gap: 15 years of nation-state effort

Agent.BTZ Fanny Flame Gauss PlugX Ramsay Retro Stuxnet USBCulprit USBferry 2021-11-18 · Cisco · Josh Pyorre

BlackMatter, LockBit, and THOR

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

ShadowPad: the masterpiece of privately sold malware in Chinese espionage

PlugX ShadowPad 2021-10-18 · NortonLifeLock · Norton Labs

Operation Exorcist - 7 Years of Targeted Attacks against the Roman Catholic Church

NewBounce PlugX Zupdax 2021-09-28 · Recorded Future · Insikt Group®

4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan

PlugX Winnti 2021-09-14 · McAfee · Christiaan Beek

Operation ‘Harvest’: A Deep Dive into a Long-term Campaign

MimiKatz PlugX Winnti 2021-09-10 · The Record · Catalin Cimpanu

Indonesian intelligence agency compromised in suspected Chinese hack

PlugX 2021-09-01 · YouTube (Black Hat) · Aragorn Tseng, Charles Li

Mem2Img: Memory-Resident Malware Detection via Convolution Neural Network

Cobalt Strike PlugX Waterbear 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 2021-07-27 · Palo Alto Networks Unit 42 · Alex Hinchliffe, Mike Harbison

THOR: Previously Unseen PlugX Variant Deployed During Microsoft Exchange Server Attacks by PKPLUG Group

PlugX 2021-07-21 · Bitdefender · Bogdan Botezatu, Victor Vrabie

LuminousMoth – PlugX, File Exfiltration and Persistence Revisited

PlugX 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 2021-06-02 · xorhex blog · Twitter (@xorhex)

RedDelta PlugX Undergoing Changes and Overlapping Again with Mustang Panda PlugX Infrastructure

PlugX 2021-06-02 · Twitter (@xorhex) · Xorhex

Tweet on new variant of PlugX from RedDelta Group

PlugX 2021-05-27 · xorhex blog · Twitter (@xorhex)

Mustang Panda PlugX - Reused Mutex and Folder Found in the Extracted Config

PlugX 2021-05-17 · xorhex blog · Twitter (@xorhex)

Mustang Panda PlugX - 45.251.240.55 Pivot

PlugX 2021-05-07 · TEAMT5 · Aragorn Tseng, Charles Li

Mem2Img: Memory-Resident Malware Detection via Convolution Neural Network

Cobalt Strike PlugX Waterbear 2021-03-29 · The Record · Catalin Cimpanu

RedEcho group parks domains after public exposure

PlugX ShadowPad RedEcho 2021-03-25 · Recorded Future · Insikt Group®

Suspected Chinese Group Calypso APT Exploiting Vulnerable Microsoft Exchange Servers

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

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

PlugX Poison Ivy TA428 2021-03-10 · ESET Research · Mathieu Tartare, Matthieu Faou, Thomas Dupuy

Exchange servers under siege from at least 10 APT groups

Microcin MimiKatz PlugX Winnti APT27 APT41 Calypso Tick ToddyCat Tonto Team Vicious Panda 2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-02-28 · Recorded Future · Insikt Group®

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

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

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

PlugX ShadowPad RedEcho 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 2021-02-08 · Myanmar Computer Emergency Response Team · Myanmar Computer Emergency Response Team

PlugX Removal Guide Version 1.2

PlugX 2021-01-20 · Trend Micro · Abraham Camba, Gilbert Sison, Ryan Maglaque

XDR investigation uncovers PlugX, unique technique in APT attack

PlugX 2021-01-15 · Swisscom · Markus Neis

Cracking a Soft Cell is Harder Than You Think

Ghost RAT MimiKatz PlugX Poison Ivy Trochilus RAT 2021-01-14 · PTSecurity · PT ESC Threat Intelligence

Higaisa or Winnti? APT41 backdoors, old and new

Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad 2021-01-09 · Marco Ramilli's Blog · Marco Ramilli

Command and Control Traffic Patterns

ostap LaZagne Agent Tesla Azorult Buer Cobalt Strike DanaBot DarkComet Dridex Emotet Formbook IcedID ISFB NetWire RC PlugX Quasar RAT SmokeLoader TrickBot 2021-01-04 · Bleeping Computer · Ionut Ilascu

China's APT hackers move to ransomware attacks

Clambling PlugX 2020-12-24 · IronNet · Adam Hlavek

China cyber attacks: the current threat landscape

PLEAD TSCookie FlowCloud Lookback PLEAD PlugX Quasar RAT Winnti 2020-12-10 · ESET Research · Mathieu Tartare

Operation StealthyTrident: corporate software under attack

HyperBro PlugX ShadowPad Tmanger 2020-12-10 · ESET Research · Mathieu Tartare

Operation StealthyTrident: corporate software under attack

HyperBro PlugX Tmanger TA428 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

Albaniiutas HyperBro PlugX PolPo Tmanger 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

Albaniiutas HyperBro PlugX Tmanger TA428 2020-11-23 · Proofpoint · Proofpoint Threat Research Team

TA416 Goes to Ground and Returns with a Golang PlugX Malware Loader

PlugX MUSTANG PANDA 2020-11-20 · Trend Micro · Abraham Camba, Bren Matthew Ebriega, Gilbert Sison

Weaponizing Open Source Software for Targeted Attacks

LaZagne Defray PlugX 2020-11-04 · Sophos · Gabor Szappanos

A new APT uses DLL side-loads to “KilllSomeOne”

KilllSomeOne PlugX 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 2020-10-27 · 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 2020-09-15 · Recorded Future · Insikt Group®

Back Despite Disruption: RedDelta Resumes Operations

PlugX 2020-09-11 · ThreatConnect · ThreatConnect Research Team

Research Roundup: Activity on Previously Identified APT33 Domains

Emotet PlugX APT33 2020-07-29 · ESET Research · welivesecurity

THREAT REPORT Q2 2020

DEFENSOR ID HiddenAd Bundlore Pirrit Agent.BTZ Cerber ClipBanker CROSSWALK Cryptowall CTB Locker DanaBot Dharma Formbook Gandcrab Grandoreiro Houdini ISFB LockBit Locky Mailto Maze Microcin Nemty NjRAT Phobos PlugX Pony REvil Socelars STOP Tinba TrickBot WannaCryptor 2020-07-29 · Recorded Future · Insikt Group

Chinese State-sponsored Group RedDelta Targets the Vatican and Catholic Organizations

PlugX 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 2020-07-28 · · NTT · NTT Security

CraftyPanda 標的型攻撃解析レポート

Ghost RAT PlugX 2020-07-20 · Risky.biz · Daniel Gordon

What even is Winnti?

CCleaner Backdoor Ghost RAT PlugX ZXShell 2020-07-20 · Dr.Web · Dr.Web

Study of the APT attacks on state institutions in Kazakhstan and Kyrgyzstan

Microcin Mirage PlugX WhiteBird 2020-07-20 · or10nlabs · oR10n

Reverse Engineering the New Mustang Panda PlugX Downloader

PlugX 2020-07-15 · ZDNet · Catalin Cimpanu

Chinese state hackers target Hong Kong Catholic Church

PlugX 2020-07-05 · or10nlabs · oR10n

Reverse Engineering the Mustang Panda PlugX RAT – Extracting the Config

PlugX 2020-07-01 · Contextis · Lampros Noutsos, Oliver Fay

DLL Search Order Hijacking

Cobalt Strike PlugX 2020-06-03 · Kaspersky Labs · Giampaolo Dedola, GReAT, Mark Lechtik

Cycldek: Bridging the (air) gap

8.t Dropper NewCore RAT PlugX USBCulprit GOBLIN PANDA Hellsing 2020-06-02 · Lab52 · Jagaimo Kawaii

Mustang Panda Recent Activity: Dll-Sideloading trojans with temporal C2 servers

PlugX 2020-05-24 · or10nlabs · oR10n

Reverse Engineering the Mustang Panda PlugX Loader

PlugX 2020-05-15 · Twitter (@stvemillertime) · Steve Miller

Tweet on SOGU development timeline, including TIGERPLUG IOCs

PlugX 2020-05-14 · Lab52 · Dex

The energy reserves in the Eastern Mediterranean Sea and a malicious campaign of APT10 against Turkey

Cobalt Strike HTran MimiKatz PlugX Quasar RAT 2020-05-01 · · Viettel Cybersecurity · Cyberthreat

Chiến dịch của nhóm APT Trung Quốc Goblin Panda tấn công vào Việt Nam lợi dụng đại dịch Covid-19 (phần 1)

NewCore RAT PlugX 2020-03-22 · Anomali · Anomali Threat Research

COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication

PlugX 2020-03-19 · · VinCSS · m4n0w4r

Analysis of malware taking advantage of the Covid-19 epidemic to spread fake "Directive of Prime Minister Nguyen Xuan Phuc" - Part 2

PlugX 2020-03-10 · · VinCSS · m4n0w4r

[RE012] Analysis of malware taking advantage of the Covid-19 epidemic to spread fake "Directive of Prime Minister Nguyen Xuan Phuc" - Part 1

PlugX 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 2020-02-21 · ADEO DFIR · ADEO DFIR

APT10 Threat Analysis Report

CHINACHOPPER HTran MimiKatz PlugX Quasar RAT 2020-02-18 · Trend Micro · Cedric Pernet, Daniel Lunghi, Jamz Yaneza, Kenney Lu

Uncovering DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations

Cobalt Strike HyperBro PlugX Trochilus RAT Operation DRBControl 2020-02-17 · Talent-Jump Technologies · Theo Chen, Zero Chen

CLAMBLING - A New Backdoor Base On Dropbox

HyperBro PlugX 2020-01-31 · Avira · Shahab Hamzeloofard

New wave of PlugX targets Hong Kong

PlugX 2020-01-31 · YouTube (Context Information Security) · Contextis

New AVIVORE threat group – how they operate and managing the risk

PlugX 2020-01-01 · Secureworks · SecureWorks

BRONZE ATLAS

Speculoos Winnti ACEHASH CCleaner Backdoor CHINACHOPPER Empire Downloader HTran MimiKatz PlugX Winnti APT41 2020-01-01 · Secureworks · SecureWorks

BRONZE EXPRESS

9002 RAT CHINACHOPPER IsSpace NewCT PlugX smac APT26 2020-01-01 · Secureworks · SecureWorks

BRONZE FIRESTONE

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

BRONZE KEYSTONE

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

BRONZE OLIVE

ANGRYREBEL PlugX APT22 2020-01-01 · Secureworks · SecureWorks

BRONZE OVERBROOK

Aveo DDKONG IsSpace PLAINTEE PlugX Rambo DragonOK 2020-01-01 · Secureworks · SecureWorks

BRONZE PRESIDENT

CHINACHOPPER Cobalt Strike PlugX MUSTANG PANDA 2020-01-01 · Secureworks · SecureWorks

BRONZE RIVERSIDE

Anel ChChes Cobalt Strike PlugX Poison Ivy Quasar RAT RedLeaves APT10 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 WOODLAND

PlugX Zeus Roaming Tiger 2020-01-01 · Dragos · Joe Slowik

Threat Intelligence and the Limits of Malware Analysis

Exaramel Exaramel Industroyer Lookback NjRAT PlugX 2019-12-29 · Secureworks · CTU Research Team

BRONZE PRESIDENT Targets NGOs

PlugX 2019-11-16 · Silas Cutler's Blog · Silas Cutler

Fresh PlugX October 2019

PlugX 2019-11-11 · Virus Bulletin · Hiroshi Soeda, Shusei Tomonaga, Tomoaki Tani, Wataru Takahashi

APT cases exploiting vulnerabilities in region-specific software

NodeRAT Emdivi PlugX 2019-10-31 · PTSecurity · PTSecurity

Calypso APT: new group attacking state institutions

BYEBY FlyingDutchman Hussar PlugX 2019-10-22 · Contextis · Contextis

AVIVORE - An overview of Tools, Techniques and Procedures (Whitepaper)

PlugX Avivore 2019-10-03 · Palo Alto Networks Unit 42 · Alex Hinchliffe

PKPLUG: Chinese Cyber Espionage Group Attacking Asia

HenBox Farseer PlugX 2019-10-03 · ComputerWeekly · Alex Scroxton

New threat group behind Airbus cyber attacks, claim researchers

PlugX Avivore 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 2019-06-19 · YouTube (44CON Information Security Conference) · Kevin O'Reilly

The Malware CAPE: Automated Extraction of Configuration and Payloads from Sophisticated Malware

PlugX 2019-06-03 · FireEye · Chi-en Shen

Into the Fog - The Return of ICEFOG APT

Icefog PlugX Sarhust 2019-05-24 · Fortinet · Ben Hunter

Uncovering new Activity by APT10

PlugX Quasar RAT 2019-03-19 · NSHC · ThreatRecon Team

SectorM04 Targeting Singapore – An Analysis

PlugX Termite 2018-12-14 · Australian Cyber Security Centre · ASD

Investigationreport: Compromise of an Australian companyvia their Managed Service Provider

PlugX RedLeaves 2018-08-21 · Trend Micro · Jaromír Hořejší, Joseph C Chen, Kawabata Kohei, Kenney Lu

Operation Red Signature Targets South Korean Companies

9002 RAT PlugX Operation Red Signature 2018-07-31 · Medium Sebdraven · Sébastien Larinier

Malicious document targets Vietnamese officials

8.t Dropper PlugX 1937CN 2018-05-09 · COUNT UPON SECURITY · Luis Rocha

Malware Analysis - PlugX - Part 2

PlugX 2018-03-13 · Kaspersky Labs · Denis Makrushin, Yury Namestnikov

Time of death? A therapeutic postmortem of connected medicine

PlugX 2018-02-04 · COUNT UPON SECURITY · Luis Rocha

MALWARE ANALYSIS – PLUGX

PlugX 2017-12-18 · · LAC · Yoshihiro Ishikawa

Relationship between PlugX and attacker group "DragonOK"

PlugX 2017-06-27 · Palo Alto Networks Unit 42 · Esmid Idrizovic, Tom Lancaster

Paranoid PlugX

PlugX 2017-05-31 · MITRE · MITRE ATT&CK

Axiom

Derusbi 9002 RAT BLACKCOFFEE Derusbi Ghost RAT HiKit PlugX ZXShell APT17 2017-04-27 · US-CERT · US-CERT

Alert (TA17-117A): Intrusions Affecting Multiple Victims Across Multiple Sectors

PlugX RedLeaves 2017-04-03 · JPCERT/CC · Shusei Tomonaga

RedLeaves - Malware Based on Open Source RAT

PlugX RedLeaves Trochilus RAT 2017-04-01 · PricewaterhouseCoopers · PricewaterhouseCoopers

Operation Cloud Hopper: Technical Annex

ChChes PlugX Quasar RAT RedLeaves Trochilus RAT 2017-02-21 · JPCERT/CC · Shusei Tomonaga

PlugX + Poison Ivy = PlugIvy? - PlugX Integrating Poison Ivy’s Code

PlugX 2017-02-13 · RSA · RSA Research

KINGSLAYER – A SUPPLY CHAIN ATTACK

CodeKey PlugX 2016-08-25 · Malwarebytes · Malwarebytes Labs

Unpacking the spyware disguised as antivirus

PlugX 2016-06-13 · · Macnica Networks · Macnica Networks

Survey of the actual situation of the large-scale cyber spy activity that hit Japan | 1st edition

Emdivi PlugX 2016-01-22 · RSA Link · Norton Santos

PlugX APT Malware

PlugX 2015-09-15 · Proofpoint · Aleksey F, Thoufique Haq

In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia

PlugX 2015-08-01 · Arbor Networks · ASERT Team

Uncovering the Seven Pointed Dagger

9002 RAT EvilGrab PlugX Trochilus RAT APT9 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 2015-01-29 · JPCERT/CC · Shusei Tomonaga

Analysis of a Recent PlugX Variant - “P2P PlugX”

PlugX 2014-06-27 · SophosLabs · Gabor Szappanos

PlugX - The Next Generation

PlugX 2014-06-10 · FireEye · Mike Scott

Clandestine Fox, Part Deux

PlugX 2014-01-06 · Airbus · Fabien Perigaud

PlugX: some uncovered points

PlugX 2013-03-29 · Computer Incident Response Center Luxembourg · CIRCL

Analysis Report (TLP:WHITE) Analysis of a PlugX variant (PlugX version 7.0)

PlugX 2013-03-26 · Contextis · Kevin O’Reilly

PlugX–Payload Extraction

PlugX 2013-02-27 · Trend Micro · Abraham Camba

BKDR_RARSTONE: New RAT to Watch Out For

PlugX Naikon 2012-02-10 · tracker.h3x.eu · Malware Corpus Tracker

Info for Family: plugx

PlugX

- [TLP:WHITE] win_plugx_auto (20251219 | Detects win.plugx.)
- [TLP:WHITE] win_plugx_w1 (20170517 | PlugX Identifying Strings)
- [TLP:WHITE] win_plugx_w2 (20170517 | PlugX RAT)
