# BazarBackdoor (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:20:10 UTC

BazarBackdoor is a small backdoor, probably by a TrickBot "spin-off" like anchor. Its called team9 backdoor (and the corresponding loader: team9 restart loader).

For now, it exclusively uses Emercoin domains (.bazar), thus the naming. FireEye uses KEGTAP as name for BazarLoader and BEERBOT for BazarBackdoor.

2023-02-03 · Mandiant · Genevieve Stark, Kimberly Goody
Float Like a Butterfly Sting Like a Bee
BazarBackdoor BumbleBee Cobalt Strike 2022-12-06 · EuRepoC · Camille Borrett, Kerstin Zettl-Schabath, Lena Rottinger
Conti/Wizard Spider
BazarBackdoor Cobalt Strike Conti Emotet IcedID Ryuk TrickBot WIZARD SPIDER 2022-11-21 · Palo Alto Networks Unit 42 · Kristopher Russo
Threat Assessment: Luna Moth Callback Phishing Campaign
BazarBackdoor Conti Luna Moth 2022-10-06 · Trellix · Daksh Kapur
Evolution of BazarCall Social Engineering Tactics
BazarBackdoor BazarCall 2022-08-06 · MalwareBookReports · muzi
A LOOK BACK AT BAZARLOADER'S DGA
BazarBackdoor 2022-08-03 · Palo Alto Networks Unit 42 · Brad Duncan
Flight of the Bumblebee: Email Lures and File Sharing Services Lead to Malware
BazarBackdoor BumbleBee Cobalt Strike Conti 2022-06-24 · Palo Alto Networks Unit 42 · Mark Lim, Riley Porter
There Is More Than One Way to Sleep: Dive Deep Into the Implementations of API Hammering by Various Malware Families
BazarBackdoor Zloader 2022-06-21 · McAfee · Lakshya Mathur
Rise of LNK (Shortcut files) Malware
BazarBackdoor Emotet IcedID QakBot 2022-06-15 · AttackIQ · AttackIQ Adversary Research Team, Jackson Wells
Attack Graph Emulating the Conti Ransomware Team's Behaviors
BazarBackdoor Conti TrickBot 2022-06-12 · cocomelonc
Malware development: persistence - part 7. Winlogon. Simple C++ example.
BazarBackdoor Gazer TurlaRPC Turla SilentMoon 2022-05-27 · 0ffset Blog · Chuong Dong
BAZARLOADER: Analysing The Main Loader
BazarBackdoor 2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker

PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT 2022-05-09 · Microsoft Security · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center

Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself

Griffon BazarBackdoor BlackCat BlackMatter Blister Gozi LockBit Pandora Rook SystemBC TrickBot 2022-04-29 · NCC Group · Mike Stokkel, Nikolaos Pantazopoulos, Nikolaos Totosis

Adventures in the land of BumbleBee – a new malicious loader

BazarBackdoor BumbleBee Conti 2022-04-25 · paloalto Networks Unit 42 · Mark Lim

Defeating BazarLoader Anti-Analysis Techniques

BazarBackdoor 2022-04-19 · 0ffset Blog · Chuong Dong

BAZARLOADER: Unpacking An ISO File Infection

BazarBackdoor 2022-04-18 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy

Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group

AvosLocker BazarBackdoor BlackByte BlackCat Cobalt Strike HelloKitty Hive Karakurt 2022-04-17 · BushidoToken Blog · BushidoToken

Lessons from the Conti Leaks

BazarBackdoor Conti Emotet IcedID Ryuk TrickBot 2022-04-15 · Bleeping Computer · Ionut Ilascu

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Anchor BazarBackdoor Conti TrickBot 2022-04-05 · Intel 471 · Intel 471

Move fast and commit crimes: Conti’s development teams mirror corporate tech

BazarBackdoor TrickBot 2022-03-30 · Prevailion · Prevailion

Wizard Spider continues to confound

BazarBackdoor Cobalt Strike Emotet 2022-03-22 · Red Canary · Red Canary

2022 Threat Detection Report

FAKEUPDATES Silver Sparrow BazarBackdoor Cobalt Strike GootKit Yellow Cockatoo RAT 2022-03-21 · eSentire · eSentire Threat Response Unit (TRU)

Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered

HelloKitty BazarBackdoor Cobalt Strike Conti FiveHands HelloKitty IcedID 2022-03-17 · Google · Benoit Sevens, Google Threat Analysis Group, Vladislav Stolyarov

Exposing initial access broker with ties to Conti

BazarBackdoor BumbleBee Cobalt Strike Conti 2022-03-17 · Trend Micro · Trend Micro Research

Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report

REvil BazarBackdoor Buer IcedID QakBot REvil 2022-03-17 · Google · Benoit Sevens, Vladislav Stolyarov

Exposing initial access broker with ties to Conti

BazarBackdoor BumbleBee Conti EXOTIC LILY 2022-03-10 · Bleeping Computer · Bill Toulas

Corporate website contact forms used to spread BazarBackdoor malware

BazarBackdoor 2022-03-09 · Bleeping Computer · Ionut Ilascu

CISA updates Conti ransomware alert with nearly 100 domain names

BazarBackdoor Cobalt Strike Conti TrickBot 2022-03-09 · Abnormal · Belem Regalado, Rachelle Chouinard

BazarLoader Actors Initiate Contact via Website Contact Forms

BazarBackdoor 2022-03-03 · Trend Micro · Trend Micro Research

Cyberattacks are Prominent in the Russia-Ukraine Conflict

BazarBackdoor Cobalt Strike Conti Emotet WhisperGate 2022-02-26 · Mandiant · Mandiant

TRENDING EVIL Q1 2022

KEYPLUG FAKEUPDATES GootLoader BazarBackdoor QakBot 2022-02-25 · CyberScoop · Joe Warminsky

TrickBot malware suddenly got quiet, researchers say, but it's hardly the end for its operators

BazarBackdoor Emotet TrickBot 2022-02-24 · kienmanowar Blog · m4n0w4r, Tran Trung Kien

[QuickNote] Techniques for decrypting BazarLoader strings

BazarBackdoor 2022-02-24 · The Hacker News · Ravie Lakshmanan

TrickBot Gang Likely Shifting Operations to Switch to New Malware

BazarBackdoor Emotet QakBot TrickBot 2022-02-24 · The Hacker News · Ravie Lakshmanan

Notorious TrickBot Malware Gang Shuts Down its Botnet Infrastructure

BazarBackdoor Emotet TrickBot 2022-02-16 · Medium elis531989 · Eli Salem

Highway to Conti: Analysis of Bazarloader

BazarBackdoor 2022-02-02 · IBM · Kevin Henson

TrickBot Gang Uses Template-Based Metaprogramming in Bazar Malware

BazarBackdoor TrickBot 2022-01-22 · forensicitguy · Tony Lambert

BazarISO Analysis - Loading with Advpack.dll

BazarBackdoor 2022-01-18 · Recorded Future · Insikt Group®

2021 Adversary Infrastructure Report

BazarBackdoor Cobalt Strike Dridex IcedID QakBot TrickBot 2022-01-15 · MalwareBookReports · muzi

BazarLoader - Back from Holiday Break

BazarBackdoor 2022-01-02 · BleepingComputer · Lawrence Abrams

Malicious CSV text files used to install BazarBackdoor malware

BazarBackdoor 2021-12-13 · The DFIR Report · The DFIR Report

Diavol Ransomware

BazarBackdoor Conti Diavol 2021-11-30 · Symantec · Symantec Threat Hunter Team

Yanluowang: Further Insights on New Ransomware Threat

BazarBackdoor Cobalt Strike FiveHands 2021-11-29 · The DFIR Report · The DFIR Report

CONTInuing the Bazar Ransomware Story

BazarBackdoor Cobalt Strike Conti 2021-11-23 · Trend Micro · Ian Kenefick

BazarLoader Adds Compromised Installers, ISO to Arrival and Delivery Vectors

BazarBackdoor 2021-11-16 · PC's Xcetra Support · David Ledbetter

Excel 4 macro code obfuscation

BazarBackdoor 2021-11-11 · SophosLabs Uncut · Andrew Brandt

BazarLoader ‘call me back’ attack abuses Windows 10 Apps mechanism

BazarBackdoor 2021-11-05 · Twitter (@Unit42_Intel) · Unit 42

Tweet on TA551 (Shathak) BazarLoader infection with CobaltStrike and DarkVNC drops

BazarBackdoor Cobalt Strike 2021-10-18 · paloalto Netoworks: Unit42 · Brad Duncan

Case Study: From BazarLoader to Network Reconnaissance

BazarBackdoor Cobalt Strike 2021-10-13 · IBM · Charlotte Hammond, Ole Villadsen

Trickbot Rising — Gang Doubles Down on Infection Efforts to Amass Network Footholds

BazarBackdoor TrickBot 2021-10-08 · Zscaler · Lenart Brave, Tarun Dewan

New Trickbot and BazarLoader campaigns use multiple delivery vectorsi

BazarBackdoor TrickBot 2021-10-07 · Mandiant · Adam Brunner, Genevieve Stark, Jennifer Brooks, Jeremy Kennelly, Joshua

Shilko, Kimberly Goody, Zach Riddle

FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets

BazarBackdoor GRIMAGENT Ryuk 2021-10-04 · The DFIR Report · The DFIR Report

BazarLoader and the Conti Leaks

BazarBackdoor Cobalt Strike Conti 2021-10-04 · Cisco · Tiago Pereira

Threat hunting in large datasets by clustering security events

BazarBackdoor TrickBot 2021-09-17 · CrowdStrike · Falcon OverWatch Team

Falcon OverWatch Hunts Down Adversaries Where They Hide

BazarBackdoor Cobalt Strike 2021-09-13 · The DFIR Report · The DFIR Report

BazarLoader to Conti Ransomware in 32 Hours

BazarBackdoor Cobalt Strike Conti 2021-09-04 · cocomelonc · cocomelonc

AV engines evasion for C++ simple malware: part 1

4h  rat Azorult BADCALL BadNews BazarBackdoor Cardinal RAT 2021-09-03 · Trend Micro · Mohamad Mokbel

The State of SSL/TLS Certificate Usage in Malware C&C Communications

AdWind ostap AsyncRAT BazarBackdoor BitRAT Buer Chthonic CloudEyE Cobalt Strike DCRat Dridex FindPOS GootKit Gozi IcedID ISFB Nanocore RAT Orcus RAT PandaBanker Qadars QakBot Quasar RAT Rockloader ServHelper Shifu SManager TorrentLocker TrickBot Vawtrak Zeus Zloader 2021-08-15 · Symantec · Threat Hunter Team

The Ransomware Threat

Babuk BlackMatter DarkSide Avaddon Babuk BADHATCH BazarBackdoor BlackMatter Clop Cobalt Strike Conti DarkSide DoppelPaymer Egregor Emotet FiveHands FriedEx Hades IcedID LockBit Maze MegaCortex MimiKatz QakBot RagnarLocker REvil Ryuk TrickBot WastedLocker 2021-08-09 · Johannes Bader's Blog · Johannes Bader

A BazarLoader DGA that Breaks Down in the Summer

BazarBackdoor 2021-08-01 · The DFIR Report · The DFIR Report

BazarCall to Conti Ransomware via Trickbot and Cobalt Strike

BazarBackdoor Cobalt Strike Conti TrickBot 2021-07-30 · Twitter (@Unit42_Intel) · Unit 42

Tweet on BazarLoader infection leading to cobaltstrike and Powershell script file for PrintNightmare vulnerability

BazarBackdoor Cobalt Strike 2021-07-30 · Medium walmartglobaltech · Jason Reaves

Decrypting BazarLoader strings with a Unicorn

BazarBackdoor 2021-07-29 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

BazaCall: Phony call centers lead to exfiltration and ransomware

BazarBackdoor Cobalt Strike 2021-07-29 · Microsoft · Microsoft Defender Threat Intelligence

BazaCall: Phony call centers lead to exfiltration and ransomware

BazarBackdoor BazarCall 2021-07-14 · Bleeping Computer · Ionut Ilascu

BazarBackdoor sneaks in through nested RAR and ZIP archives

BazarBackdoor 2021-06-16 · Proofpoint · Daniel Blackford, Garrett M. Graff, Selena Larson

The First Step: Initial Access Leads to Ransomware

BazarBackdoor Egregor IcedID Maze QakBot REvil Ryuk TrickBot WastedLocker TA570 TA575 TA577 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 2021-05-19 · Palo Alto Networks

Unit 42 · Brad Duncan

BazarCall: Call Centers Help Spread BazarLoader Malware

BazarBackdoor campoloader 2021-05-11 · Mal-Eats · mal_eats

Campo, a New Attack Campaign Targeting Japan

AnchorDNS BazarBackdoor campoloader Cobalt Strike Phobos Snifula TrickBot Zloader 2021-05-10 · Mal-Eats · mal_eats

Overview of Campo, a new attack campaign targeting Japan

AnchorDNS BazarBackdoor Cobalt Strike ISFB Phobos TrickBot Zloader 2021-04-15 · SophosLabs Uncut · Andrew Brandt

BazarLoader deploys a pair of novel spam vectors

BazarBackdoor 2021-04-14 · InfoSec Handlers Diary Blog · Brad Duncan

April 2021 Forensic Quiz: Answers and Analysis

Anchor BazarBackdoor Cobalt Strike 2021-04-12 · Trend Micro · Don Ovid Ladores, Frankylnn Uy, Junestherry Salvador, Lala Manly, Raphael Centeno

A Spike in BazarCall and IcedID Activity Detected in March

BazarBackdoor IcedID 2021-04-06 · Intel 471 · Intel 471

EtterSilent: the underground's new favorite maldoc builder

BazarBackdoor ISFB QakBot TrickBot 2021-03-30 · YouTube ( malware-traffic-analysis.net) · Brad Duncan

2021-03-29 BazaCall (BazarCall) Example

BazarBackdoor 2021-03-30 · FR3D.HK · Fred HK

Campo Loader - Simple but effective

BazarBackdoor 2021-03-21 · Blackberry · Blackberry Research

2021 Threat Report

Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader TrickBot 2021-03-08 · The DFIR Report · The DFIR Report

Bazar Drops the Anchor

Anchor BazarBackdoor Cobalt Strike 2021-03-01 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Nimar Loader

BazarBackdoor BazarNimrod Cobalt Strike 2021-03-01 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Ransomware Uncovered 2020/2021

RansomEXX BazarBackdoor Buer Clop Conti DoppelPaymer Dridex Egregor IcedID Maze PwndLocker QakBot RansomEXX REvil Ryuk SDBbot TrickBot Zloader 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 2021-02-25 · ANSSI · CERT-FR

Ryuk Ransomware

BazarBackdoor Buer Conti Emotet Ryuk TrickBot 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 2021-02-12 · Fortinet · Xiaopeng Zhang

New Bazar Trojan Variant is Being Spread in Recent Phishing Campaign – Part I
BazarBackdoor 2021-02-12 · Fortinet · Xiaopeng Zhang

New Bazar Trojan Variant is Being Spread in Recent Phishing Campaign – Part II
BazarBackdoor 2021-02-11 · Proofpoint · Proofpoint Threat Research Team

A Baza Valentine’s Day
BazarBackdoor 2021-02-09 · Cofense · Zachary Bailey

BazarBackdoor’s Stealthy Infiltration Evades Multiple SEGs
BazarBackdoor 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware
Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-02-01 · GoSecure · Lilly Chalupowski

BazarLoader Mocks Researchers in December 2020 Malspam Campaign
BazarBackdoor 2021-01-31 · The DFIR Report · The DFIR Report

Bazar, No Ryuk?
BazarBackdoor Cobalt Strike Ryuk 2021-01-28 · Hornetsecurity · Hornetsecurity Security Lab

BazarLoader’s Elaborate Flower Shop Lure
BazarBackdoor 2021-01-28 · Huntress Labs · John Hammond

Analyzing Ryuk Another Link in the Cyber Attack Chain
BazarBackdoor Ryuk 2021-01-23 · Johannes Bader's Blog · Johannes Bader

Yet Another Bazar Loader DGA
BazarBackdoor 2021-01-12 · Cybereason · Lior Rochberger

Cybereason vs. Conti Ransomware
BazarBackdoor Conti 2021-01-12 · Minerva Labs · MinervaLabs

Slamming The Backdoor On BazarLoader
BazarBackdoor 2021-01-06 · DomainTools · Joe Slowik

Holiday Bazar: Tracking a TrickBot-Related Ransomware Incident
BazarBackdoor TrickBot 2020-12-16 · Johannes Bader's Blog · Johannes Bader

Next Version of the Bazar Loader DGA
BazarBackdoor 2020-12-10 · Cybereason · Joakim Kandefelt

Cybereason vs. Ryuk Ransomware
BazarBackdoor Ryuk TrickBot 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away
Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-10 · Intel 471 · Intel 471

Trickbot down, but is it out?

BazarBackdoor TrickBot 2020-11-09 · Area 1 · Threat Research Team

Phishing Campaign Threatens Job Security, Drops Bazar and Buer Malware

BazarBackdoor Buer 2020-11-06 · Advanced Intelligence · Vitali Kremez

Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware "one" Group via Cobalt Strike

BazarBackdoor Cobalt Strike Ryuk 2020-11-05 · The DFIR Report · The DFIR Report

Ryuk Speed Run, 2 Hours to Ransom

BazarBackdoor Cobalt Strike Ryuk 2020-11-05 · SCYTHE · Jorge Orchilles, Sean Lyngaas

#ThreatThursday - Ryuk

BazarBackdoor Ryuk 2020-11-04 · VMRay · Giovanni Vigna

Trick or Threat: Ryuk ransomware targets the health care industry

BazarBackdoor Cobalt Strike Ryuk TrickBot 2020-10-30 · Cofense · The Cofense Intelligence Team

The Ryuk Threat: Why BazarBackdoor Matters Most

BazarBackdoor Ryuk 2020-10-30 · Github (ThreatConnect-Inc) · ThreatConnect

UNC 1878 Indicators from Threatconnect

BazarBackdoor Cobalt Strike Ryuk 2020-10-29 · Palo Alto Networks Unit 42 · Brad Duncan, Brittany Barbehenn, Doel Santos

Threat Assessment: Ryuk Ransomware and Trickbot Targeting U.S. Healthcare and Public Health Sector

Anchor BazarBackdoor Ryuk TrickBot 2020-10-29 · Twitter (@anthomsec) · Andrew Thompson

Tweet on UNC1878 activity

BazarBackdoor Ryuk TrickBot UNC1878 2020-10-28 · FireEye · Douglas Bienstock, Jeremy Kennelly, Joshua Shilko, Kimberly Goody, Steve Elovitz

Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

BazarBackdoor Cobalt Strike Ryuk UNC1878 2020-10-28 · CISA · CISA, FBI, HHS

AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector

AnchorDNS Anchor BazarBackdoor Ryuk 2020-10-18 · The DFIR Report · The DFIR Report

Ryuk in 5 Hours

BazarBackdoor Cobalt Strike Ryuk 2020-10-16 · CrowdStrike · The Crowdstrike Intel Team

WIZARD SPIDER Update: Resilient, Reactive and Resolute

BazarBackdoor Conti Ryuk TrickBot 2020-10-13 · Hornetsecurity · Security Lab

BazarLoader Campaign with Fake Termination Emails

BazarBackdoor 2020-10-12 · Advanced Intelligence · Roman Marshanski, Vitali Kremez

"Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon

BazarBackdoor Cobalt Strike Ryuk 2020-10-08 · The DFIR Report · The DFIR Report

Ryuk’s Return

BazarBackdoor Cobalt Strike Ryuk 2020-10-02 · Health Sector Cybersecurity Coordination Center (HC3) · Health Sector Cybersecurity Coordination Center (HC3)

Report 202010021600: Recent Bazarloader Use in Ransomware Campaigns

BazarBackdoor Cobalt Strike Ryuk TrickBot 2020-09-29 · Zscaler · Atinderpal Singh, Mohd Sadique

Spear Phishing Campaign Delivers Buer and Bazar Malware

BazarBackdoor Buer 2020-07-16 · Cybereason · Assaf Dahan, Daniel Frank, Mary Zhao

A Bazar of Tricks: Following Team9’s Development Cycles

BazarBackdoor 2020-07-16 · Cybereason · Assaf Dahan, Daniel Frank, Mary Zhao

A Bazar of Tricks: Following Team9’s Development Cycles (IOCs)

BazarBackdoor 2020-07-15 · Johannes Bader's Blog · Johannes Bader

The Defective Domain Generation Algorithm of BazarBackdoor

BazarBackdoor 2020-07-14 · Johannes Bader's Blog · Johannes Bader

The Domain Generation Algorithm of BazarBackdoor

BazarBackdoor 2020-06-02 · NCC Group · Nikolaos Pantazopoulos, Stefano Antenucci

In-depth analysis of the new Team9 malware family

BazarBackdoor 2020-06-02 · Fox-IT · NCC RIFT, Nikolaos Pantazopoulos, Stefano Antenucci

In-depth analysis of the new Team9 malware family

BazarBackdoor 2020-05-19 · AlienLabs · Ofer Caspi

TrickBot BazarLoader In-Depth

Anchor BazarBackdoor TrickBot 2020-04-27 · Trend Micro · Trend Micro

Group Behind TrickBot Spreads Fileless BazarBackdoor

BazarBackdoor 2020-04-24 · Vitali Kremez

TrickBot "BazarBackdoor" Process Hollowing Injection Primer

BazarBackdoor 2020-04-24 · Bleeping Computer · Lawrence Abrams

BazarBackdoor: TrickBot gang’s new stealthy network-hacking malware

BazarBackdoor

▶ [TLP:WHITE] win_bazarbackdoor_auto (20251219 | Detects win.bazarbackdoor.)

---