QakBot (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:07:18 UTC

QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.

2024-07-29 · Mandiant · Ashley Pearson, Jake Nicastro, Joseph Pisano, Josh Murchie, Joshua Shilko, Raymond Leong
UNC4393 Goes Gently into the SILENTNIGHT
Black Basta QakBot sRDI SystemBC Zloader UNC3973 UNC4393 2024-07-09 · Spamhaus ·
Spamhaus Botnet Threat Update January to June 2024
Coper FluBot Hook Bashlite Mirai FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc NjRAT
QakBot Quasar RAT RedLine Stealer Remcos Rhadamanthys RisePro Sliver 2024-05-26 · ZW01f · Mohamed Ezat
QakBOT v5 Deep Malware Analysis
QakBot 2024-05-15 · Microsoft · Microsoft Threat Intelligence
Threat actors misusing Quick Assist in social engineering attacks leading to ransomware
Black Basta Cobalt Strike QakBot UNC4393 2024-05-15 · X (@bryceabdo) · Bryce Abdo
Tweet on UNC5449 exploiting CVE-2024-30051 to deliver QAKBOT
QakBot 2024-05-15 · Microsoft · Microsoft Threat Intelligence
Threat actors misusing Quick Assist in social engineering attacks leading to ransomware
Black Basta Cobalt Strike QakBot SystemBC 2024-05-14 · Kaspersky · Boris Larin, Mert Degirmenci
QakBot attacks with Windows zero-day (CVE-2024-30051)
Cobalt Strike QakBot 2024-04-24 · kienmanowar Blog · m4n0w4r, Tran Trung Kien
[QuickNote] Qakbot 5.0 – Decrypt strings and configuration
QakBot 2024-02-28 · Security Intelligence · Golo Mühr, Ole Villadsen
X-Force data reveals top spam trends, campaigns and senior superlatives in 2023
404 Keylogger Agent Tesla Black Basta DarkGate Formbook IcedID Loki Password Stealer (PWS) Pikabot
QakBot Remcos 2024-02-21 · YouTube (Invoke RE) · Josh Reynolds
Analyzing Qakbot Using Binary Ninja Automation Part 3
QakBot 2024-02-21 · Invoke RE · Josh Reynolds
Automating Qakbot Malware Analysis with Binary Ninja
QakBot 2024-02-16 · Malcat · malcat team
Writing a Qakbot 5.0 config extractor with Malcat
QakBot 2024-02-09 · Censys · Censys, Embee_research
A Beginners Guide to Tracking Malware Infrastructure
AsyncRAT BianLian Cobalt Strike QakBot 2024-02-09 · YouTube (Invoke RE) · Josh Reynolds
Analyzing and Unpacking Qakbot Using Binary Ninja Automation Part 2
QakBot 2024-01-31 · Zscaler · Javier Vicente
Tracking 15 Years of Qakbot Development

QakBot 2024-01-23 · YouTube (Invoke RE) · Josh Reynolds

Analyzing and Unpacking Qakbot using Binary Ninja Automation

QakBot 2024-01-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q4 2023

FluBot Hook FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc IcedID Lumma Stealer Meterpreter NjRAT Pikabot QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver 2024-01-12 · YouTube (BSides Cambridge UK) · Cian Heasley

Slipping The Net: Qakbot, Emotet And Defense Evasion

Emotet QakBot 2024-01-04 · K7 Security · Saikumaravel

Qakbot Returns

QakBot 2023-12-05 · YouTube (SecureWorks) · Austin Graham

Emulating Qakbot with Austin Graham

QakBot 2023-11-30 · Twitter (@embee_research) · Embee_research

Advanced Threat Intel Queries - Catching 83 Qakbot Servers with Regex, Censys and TLS Certificates

QakBot 2023-11-22 · Twitter (@embee_research) · Embee_research

Practical Queries for Malware Infrastructure - Part 3 (Advanced Examples)

BianLian Xtreme RAT NjRAT QakBot RedLine Stealer Remcos 2023-11-20 · Cofense · Dylan Duncan

Are DarkGate and PikaBot the new QakBot?

DarkGate Pikabot QakBot 2023-10-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2023

FluBot AsyncRAT Ave Maria Cobalt Strike DCRat Havoc IcedID ISFB Nanocore RAT NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Stealc Tofsee Vidar 2023-10-05 · Talos · Guilherme Venere

Qakbot-affiliated actors distribute Ransom Knight malware despite infrastructure takedown

QakBot 2023-09-11 · Github (m4now4r) · m4n0w4r

Unveiling Qakbot Exploring one of the Most Active Threat Actors

QakBot 2023-08-29 · The Shadowserver Foundation · Shadowserver Foundation

Qakbot Botnet Disruption

QakBot 2023-08-29 · US Department of Justice · US Department of Justice

Qakbot Malware Disrupted in International Cyber Takedown

QakBot 2023-08-29 · Secureworks · Counter Threat Unit ResearchTeam

Law Enforcement Takes Down QakBot

QakBot 2023-08-29 · US Department of Justice · Department of Justice

Documents and Resources related to the Disruption of the QakBot Malware and Botnet

QakBot 2023-08-29 · FBI · FBI

FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown

QakBot 2023-08-29 · KrebsOnSecurity · Brian Krebs

U.S. Hacks QakBot, Quietly Removes Botnet Infections

QakBot 2023-08-29 · Spamhaus · Spamhaus Team

Qakbot - the takedown and the remediation

QakBot 2023-08-23 · Department of Justice · United States District Court for the Central District of California

Application and Affidavit for a Seizure Warrant by Telephone or other Reliable Electronic Means

QakBot 2023-08-21 · Department of Justice · United States District Court for the Central District of California

Application for a Warrant by Telephone or other reliable Electronic Means

QakBot 2023-08-07 · Team Cymru · S2 Research Team

Visualizing Qakbot Infrastructure Part II: Uncharted Territory

QakBot 2023-07-31 · d01a · Mohamed Adel

Pikabot deep analysis

Pikabot QakBot 2023-07-28 · Red Canary · Stef Rand

Drop It Like It's Qbot: Separating malicious droppers, loaders, and crypters from their payloads

CloudEyE QakBot 2023-07-28 · YouTube (SANS Cyber Defense) · Stef Rand

Drop It Like It's Qbot: Separating malicious droppers, loaders, and crypters from their payloads

CloudEyE QakBot 2023-07-25 · Zscaler · Meghraj Nandanwar, Pradeep Mahato, Satyam Singh

Hibernating Qakbot: A Comprehensive Study and In-depth Campaign Analysis

QakBot 2023-07-11 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q2 2023

Hydra AsyncRAT Aurora Stealer Ave Maria BumbleBee Cobalt Strike DCRat Havoc IcedID ISFB NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee 2023-06-08 · Twitter (@embee_research) · Embee_research

Practical Queries for Identifying Malware Infrastructure: An informal page for storing Censys/Shodan queries

Amadey AsyncRAT Cobalt Strike QakBot Quasar RAT Sliver solarmarker 2023-06-01 · Lumen · Black Lotus Labs

Qakbot: Retool, Reinfect, Recycle

QakBot 2023-05-21 · Github (0xThiebaut) · Maxime Thiebaut

PCAPeek

IcedID QakBot 2023-05-17 · Team Cymru · Team Cymru

Visualizing QakBot Infrastructure

QakBot 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 2023-04-18 · Rapid7 Labs · Matt Green

Automating Qakbot Detection at Scale With Velociraptor

QakBot 2023-04-13 · Sublime · Sam Scholten

Detecting QakBot: WSF attachments, OneNote files, and generic attack surface reduction

QakBot 2023-04-12 · loginsoft · Bhargav koduru

Maximizing Threat Detections of Qakbot with Osquery

QakBot 2023-04-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q1 2023

FluBot Amadey AsyncRAT Aurora Ave Maria BumbleBee Cobalt Strike DCRat Emotet IcedID ISFB NjRAT QakBot RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee Vidar 2023-04-10 · Check Point · Check Point

March 2023’s Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files

Agent Tesla CloudEyE Emotet Formbook Nanocore RAT NjRAT QakBot Remcos Tofsee 2023-04-05 · velociraptor ·

Matt Green

Automating Qakbot Decode At Scale

QakBot 2023-03-30 · loginsoft · Saharsh Agrawal

From Innocence to Malice: The OneNote Malware Campaign Uncovered

Agent Tesla AsyncRAT DOUBLEBACK Emotet Formbook IcedID NetWire RC QakBot Quasar RAT RedLine Stealer XWorm 2023-03-30 · United States District Court (Eastern District of New York) · Fortra, HEALTH-ISAC, Microsoft

Cracked Cobalt Strike (1:23-cv-02447)

Black Basta BlackCat LockBit RagnarLocker LockBit Black Basta BlackCat Cobalt Strike Cuba Emotet LockBit Mount Locker PLAY QakBot RagnarLocker Royal Ransom Zloader 2023-03-24 · Lab52 · peko

Bypassing Qakbot Anti-Analysis

QakBot 2023-03-15 · Reliaquest · RELIAQUEST THREAT RESEARCH TEAM

QBot: Laying the Foundations for Black Basta Ransomware Activity

Black Basta QakBot 2023-03-07 · Trellix · Alejandro Houspanossian, John Fokker, Mathanraj Thangaraju, Pham Duy Phuc, Raghav Kapoor

Qakbot Evolves to OneNote Malware Distribution

QakBot 2023-03-02 · Netresec · Erik Hjelmvik

QakBot C2 Traffic

QakBot 2023-03-02 · Youtube (Microsoft Security Response Center (MSRC)) · Ben Magee, Daniel Taylor

BlueHat 2023: Hunting Qakbot with Daniel Taylor & Ben Magee

QakBot 2023-03-01 · Zscaler · Meghraj Nandanwar, Shatak Jain

OneNote: A Growing Threat for Malware Distribution

AsyncRAT Cobalt Strike IcedID QakBot RedLine Stealer 2023-02-24 · Medium walmartglobaltech · Jason Reaves, Jonathan Mccay, Joshua Platt, Kirk Sayre

Qbot testing malvertising campaigns?

QakBot 2023-02-17 · cyble · Cyble

The Many Faces of Qakbot Malware: A Look at Its Diverse Distribution Methods

QakBot 2023-02-14 · · DSIH · Charles Blanc-Rolin

Comment Qbot revient en force avec OneNote ?

QakBot 2023-02-06 · Sophos · Andrew Brandt

Qakbot mechanizes distribution of malicious OneNote notebooks

QakBot 2023-01-23 · Kroll · Elio Biasiotto, Stephen Green

Black Basta – Technical Analysis

Black Basta Cobalt Strike MimiKatz QakBot SystemBC 2023-01-19 · Cisco · Guilherme Venere

Following the LNK metadata trail

BumbleBee PhotoLoader QakBot 2023-01-12 · EclecticIQ · EclecticIQ Threat Research Team

QakBot Malware Used Unpatched Vulnerability to Bypass Windows OS Security Feature

QakBot 2022-12-28 · Micah Babinski

HTML Smuggling Detection

QakBot 2022-12-22 · AhnLab · ASEC

Qakbot Being Distributed via Virtual Disk Files (*.vhd)

QakBot 2022-12-05 · Cybereason · Kotaro Ogino, Ralph Villanueva, Robin Plumer

Threat Analysis: MSI - Masquerading as a Software Installer

Magniber Matanbuchus QakBot 2022-12-02 · Github (binref) · Jesko Hüttenhain

The Refinery Files 0x06: Qakbot Decoder

QakBot 2022-12-01 · splunk · Splunk Threat Research Team

From Macros to No Macros: Continuous Malware Improvements by QakBot

QakBot 2022-11-30 · Tidal Cyber Inc. · Scott Small

Identifying and Defending Against QakBot's Evolving TTPs

QakBot 2022-11-23 · Cybereason · Cybereason Global SOC Team

THREAT ALERT: Aggressive Qakbot Campaign and the Black Basta Ransomware Group Targeting U.S. Companies

Black Basta QakBot 2022-11-14 · Twitter (@embee_research) · Matthew

Twitter thread on Yara Signatures for Qakbot Encryption Routines

IcedID QakBot 2022-11-10 · Intezer · Nicole Fishbein

How LNK Files Are Abused by Threat Actors

BumbleBee Emotet Mount Locker QakBot 2022-11-03 · SentinelOne · SentinelLabs

Black Basta Ransomware | Attacks deploy Custom EDR Evasion Tools tied to FIN7 Threat Actor

Black Basta QakBot SocksBot 2022-10-31 · Security homework · Christophe Rieunier

QakBot CCs prioritization and new record types

QakBot 2022-10-31 · Cynet · Max Malyutin

Orion Threat Alert: Qakbot TTPs Arsenal and the Black Basta Ransomware

Black Basta Cobalt Strike QakBot 2022-10-13 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2022

FluBot Arkei Stealer AsyncRAT Ave Maria BumbleBee Cobalt Strike DCRat Dridex Emotet Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT QakBot RecordBreaker RedLine Stealer Remcos Socelars Tofsee Vjw0rm 2022-10-13 · Syrion · Raffaele Sabato

QAKBOT BB Configuration and C2 IPs List

QakBot 2022-10-12 · Trend Micro · Ian Kenefick, Lucas Silva, Nicole Hernandez

Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike

Black Basta Brute Ratel C4 Cobalt Strike QakBot 2022-09-06 · Zscaler · Brett Stone-Gross

The Ares Banking Trojan Learns Old Tricks: Adds the Defunct Qakbot DGA

Ares QakBot 2022-09-01 · Trend Micro · Trend Micro

Ransomware Spotlight Black Basta

Black Basta Cobalt Strike MimiKatz QakBot 2022-08-25 · Palo Alto Networks Unit 42 · Amer Elsad

Threat Assessment: Black Basta Ransomware

Black Basta QakBot 2022-08-24 · Trellix · Adithya Chandra, Sushant Kumar Arya

Demystifying Qbot Malware

QakBot 2022-08-24 · Elastic · Cyril François

QBOT Malware Analysis

QakBot 2022-07-27 · Elastic · Cyril François, Derek Ditch

QBOT Configuration Extractor

QakBot 2022-07-27 · Elastic · Andrew Pease, Cyril François, Seth Goodwin

Exploring the QBOT Attack Pattern

QakBot 2022-07-27 · cyble · Cyble Research Labs

Targeted Attacks Being Carried Out Via DLL SideLoading

Cobalt Strike QakBot 2022-07-24 · Bleeping Computer · Bill Toulas

QBot phishing uses Windows Calculator sideloading to infect devices

QakBot 2022-07-19 · Fortinet · Xiaopeng Zhang

New Variant of QakBot Being Spread by HTML File Attached to Phishing Emails

QakBot 2022-07-17 · Resecurity · Resecurity

Shortcut-Based (LNK) Attacks Delivering Malicious Code On The Rise

AsyncRAT BumbleBee Emotet IcedID QakBot 2022-07-12 · Zscaler · Aditya Sharma, Tarun Dewan

Rise in Qakbot attacks traced to evolving threat techniques

QakBot 2022-07-07 · Fortinet · Erin Lin

Notable Droppers Emerge in Recent Threat Campaigns

BumbleBee Emotet PhotoLoader QakBot 2022-07-05 · Soc Investigation · Priyadharshini Balaji

QBot Spreads via LNK Files – Detection & Response

QakBot 2022-06-30 · Trend Micro · Emmanuel Panopio, James Panlilio, John Kenneth Reyes, Kenneth Adrian Apostol, Melvin Singwa, Mirah Manlapig, Paolo Ronniel Labrador

Black Basta Ransomware Operators Expand Their Attack Arsenal With QakBot Trojan and PrintNightmare Exploit

Black Basta Cobalt Strike QakBot 2022-06-21 · McAfee · Lakshya Mathur

Rise of LNK (Shortcut files) Malware

BazarBackdoor Emotet IcedID QakBot 2022-06-17 · Github (NtQuerySystemInformation) · Twitter (@kasua02)

A reverse engineer primer on Qakbot Dll Stager: From initial execution to multithreading.

QakBot 2022-06-09 · InfoSec Handlers Diary Blog · Brad Duncan

TA570 Qakbot (Qbot) tries CVE-2022-30190 (Follina) exploit (ms-msdt)

QakBot 2022-06-02 · Mandiant · Mandiant

TRENDING EVIL Q2 2022

CloudEyE Cobalt Strike CryptBot Emotet IsaacWiper QakBot 2022-05-24 · BitSight · BitSight, João Batista, Pedro Umbelino

Emotet Botnet Rises Again

Cobalt Strike Emotet QakBot SystemBC 2022-05-19 · Trend Micro · Adolph Christian Silverio, Jeric Miguel Abordo, Khristian Joseph Morales, Maria Emreen Viray

Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware

Emotet QakBot 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 2022-04-28 · Symantec · Karthikeyan C Kasiviswanathan, Vishal Kamble

Ransomware: How Attackers are Breaching Corporate Networks

AvosLocker Conti Emotet Hive IcedID PhotoLoader QakBot TrickBot 2022-04-26 · Intel 471 · Intel 471

Conti and Emotet: A constantly destructive duo

Cobalt Strike Conti Emotet IcedID QakBot TrickBot 2022-04-20 · SANS ISC · Brad Duncan

'aa' distribution Qakbot (Qbot) infection with DarkVNC traffic

QakBot 2022-04-17 · Malwarology · Gaetano Pellegrino

Qakbot Series: API Hashing

QakBot 2022-04-16 · Malwarology · Gaetano Pellegrino

Qakbot Series: Process Injection

QakBot 2022-04-13 · Malwarology · Gaetano Pellegrino

Qakbot Series: Configuration Extraction

QakBot 2022-04-12 · Tech Times · Joseph Henry

Qbot Botnet Deploys Malware Payloads Through Malicious Windows Installers

QakBot 2022-04-11 · Bleeping Computer · Sergiu Gatlan

Qbot malware switches to new Windows Installer infection vector

QakBot 2022-04-10 · Malwarology · Gaetano Pellegrino

Qakbot Series: String Obfuscation

QakBot 2022-03-31 · nccgroup · Alex Jessop, Nikolaos Pantazopoulos, RIFT: Research and Intelligence Fusion Team, Simon Biggs

Conti-nuation: methods and techniques observed in operations post the leaks

Cobalt Strike Conti QakBot 2022-03-25 · SANS ISC · Xavier Mertens

XLSB Files: Because Binary is Stealthier Than XML

QakBot 2022-03-17 · Trend Micro · Trend Micro Research

Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report

REvil BazarBackdoor Buer IcedID QakBot REvil 2022-03-16 · SANS ISC · Brad Duncan

Qakbot infection with Cobalt Strike and VNC activity

Cobalt Strike QakBot 2022-03-16 · InfoSec Handlers Diary Blog · Brad Duncan

Qakbot infection with Cobalt Strike and VNC activity

Cobalt Strike QakBot 2022-02-26 · LinkedIn (Zayed AlJaberi) · Zayed AlJaberi

Hunting Recent QakBot Malware

QakBot 2022-02-26 · Mandiant · Mandiant

TRENDING EVIL Q1 2022

KEYPLUG FAKEUPDATES GootLoader BazarBackdoor QakBot 2022-02-24 · The Hacker News · Ravie Lakshmanan

TrickBot Gang Likely Shifting Operations to Switch to New Malware

BazarBackdoor Emotet QakBot TrickBot 2022-02-21 · The DFIR Report

Qbot and Zerologon Lead To Full Domain Compromise

Cobalt Strike QakBot 2022-02-16 · SOC Prime · Alla Yurchenko

QBot Malware Detection: Old Dog New Tricks

QakBot 2022-02-10 · Cybereason · Cybereason Global SOC Team

Threat Analysis Report: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot

Cobalt Strike Emotet IcedID QakBot 2022-02-08 · BleepingComputer · Bill Toulas

Qbot needs only 30 minutes to steal your credentials, emails

QakBot 2022-02-07 · The DFIR Report · The DFIR Report

Qbot Likes to Move It, Move It

QakBot 2022-01-19 · Blackberry · The BlackBerry Research & Intelligence Team

Kraken the Code on Prometheus

Prometheus Backdoor BlackMatter Cerber Cobalt Strike DCRat Ficker Stealer QakBot REvil Ryuk 2022-01-18 · Recorded Future · Insikt Group®

2021 Adversary Infrastructure Report

BazarBackdoor Cobalt Strike Dridex IcedID QakBot TrickBot 2022-01-15 · Atomic Matryoshka · z3r0day_504

Malware Headliners: Qakbot

QakBot 2022-01-13 · Trustwave · Lloyd Macrohon, Rodel Mendrez

Decrypting Qakbot’s Encrypted Registry Keys

QakBot 2022-01-11 · Cybereason · Chen Erlich, Daichi Shimabukuro, Niv Yona, Ofir Ozer, Omri Refaeli

Threat Analysis Report: DatopLoader Exploits ProxyShell to Deliver QBOT and Cobalt Strike

Cobalt Strike QakBot Squirrelwaffle 2021-12-17 · Trend Micro · Abraham Camba, Gilbert Sison, Jay Yaneza, Jonna Santos

Staging a Quack: Reverse Analyzing a Fileless QAKBOT Stager

QakBot 2021-12-16 · Red Canary · The Red Canary Team

Intelligence Insights: December 2021

Cobalt Strike QakBot Squirrelwaffle 2021-12-11 · YouTube (AGDC Services) · AGDC Services

How To Extract & Decrypt Qbot Configs Across Variants

QakBot 2021-12-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

A closer look at Qakbot’s latest building blocks (and how to knock them down)

QakBot 2021-11-21 · Twitter (@tylabs) · Twitter (@ffforward), Tyler McLellan

Twitter Thread about UNC1500 phishing using QAKBOT

QakBot 2021-11-19 · Trend Micro · Abdelrhman Sharshar, Mohamed Fahmy, Sherif Magdy

Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains

Cobalt Strike QakBot Squirrelwaffle 2021-11-18 · Red Canary · The Red Canary Team

Intelligence Insights: November 2021

Andromeda Conti LockBit QakBot Squirrelwaffle 2021-11-17 · Twitter (@Unit42_Intel) · Unit 42

Tweet on Matanbuchus Loader used to deliver Qakbot (tag obama128b) and follow-up CobaltStrike

Cobalt Strike QakBot 2021-11-16 · Twitter (@kienbigmummy) · m4n0w4r

Tweet on short analysis of QakBot

QakBot 2021-11-15 · TRUESEC · Fabio Viggiani

ProxyShell, QBot, and Conti Ransomware Combined in a Series of Cyberattacks

Cobalt Strike Conti QakBot 2021-11-13 · Trend Micro · Ian Kenefick, Vladimir Kropotov

QAKBOT Loader Returns With New Techniques and Tools

QakBot 2021-11-13 · YouTube (AGDC Services) · AGDC Services

Automate Qbot Malware String Decryption With Ghidra Script

QakBot 2021-11-12 · Recorded Future · Insikt Group®

The Business of Fraud: Botnet Malware Dissemination

Mozi Dridex IcedID QakBot TrickBot 2021-11-12 · Trend Micro · Ian Kenefick, Vladimir Kropotov

The Prelude to Ransomware: A Look into Current QAKBOT Capabilities and Global Activities

QakBot 2021-11-11 · Cynet · Max Malyutin

A Duck Nightmare Quakbot Strikes with QuakNightmare Exploitation

Cobalt Strike QakBot 2021-11-11 · vmware · Giovanni Vigna, Jason Zhang, Stefano Ortolani, Threat Analysis Unit

Research Recap: How To Automate Malware Campaign Detection With Telemetry Peak Analyzer

Phorpiex QakBot 2021-11-10 · CIRCL · CIRCL

TR-64 - Exploited Exchange Servers - Mails with links to malware from known/valid senders

QakBot 2021-11-09 · MinervaLabs · Minerva Labs

A New DatopLoader Delivers QakBot Trojan

QakBot Squirrelwaffle 2021-11-03 · Team Cymru · tcblogposts

Webinject Panel Administration: A Vantage Point into Multiple Threat Actor Campaigns - A Case Study on the Value of Threat Reconnaisance

DoppelDridex IcedID QakBot Zloader 2021-11-03 · Twitter (@Corvid_Cyber) · CORVID

Tweet on a unique Qbot debugger dropped by an actor after compromise

QakBot 2021-10-26 · Cisco Talos · Edmund Brumaghin, Mariano Graziano, Nick Mavis

SQUIRRELWAFFLE Leverages malspam to deliver Qakbot, Cobalt Strike

Cobalt Strike QakBot Squirrelwaffle 2021-10-26 · ANSSI

Identification of a new cyber criminal group: Lockean

Cobalt Strike DoppelPaymer Egregor Maze PwndLocker QakBot REvil 2021-10-07 · Netskope · Ghanashyam Satpathy, Gustavo Palazolo

SquirrelWaffle: New Malware Loader Delivering Cobalt Strike and QakBot

Cobalt Strike QakBot Squirrelwaffle 2021-09-03 · IBM · Andrew Gorecki, Camille Singleton, John Dwyer

Dissecting Sodinokibi Ransomware Attacks: Bringing Incident Response and Intelligence Together in the Fight

Valak QakBot REvil 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 2021-09-02 · Kaspersky · Anton Kuzmenko, Haim Zigel, Oleg Kupreev

QakBot Technical Analysis

QakBot 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 2021-08-05 · Group-IB · Nikita Rostovcev, Viktor Okorokov

Prometheus TDS The key to success for Campo Loader, Hancitor, IcedID, and QBot

Prometheus Backdoor Buer campoloader Hancitor IcedID QakBot 2021-08-05 · The Record · Catalin Cimpanu

Meet Prometheus, the secret TDS behind some of today's malware campaigns

Buer campoloader IcedID QakBot 2021-07-30 · HP · Patrick Schläpfer

Detecting TA551 domains

Valak Dridex IcedID ISFB QakBot 2021-07-24 · 0ffset Blog · Daniel Bunce

Quack Quack: Analysing Qakbot's Browser Hooking Module – Part 1

QakBot 2021-06-24 · Kaspersky · Anton Kuzmenko

Malicious spam campaigns delivering banking Trojans

IcedID QakBot 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 2021-06-

16 · Twitter (@ChouchWard) · ch0uch ward

Tweet on Qbot operators left their web server's access.log file unsecured

QakBot 2021-06-16 · · S2 Grupo · CSIRT-CV (the ICT Security Center of the Valencian Community)

Emotet campaign analysis

Emotet QakBot 2021-06-15 · Perception Point · Shai Golderman

Insights Into an Excel 4.0 Macro Attack using Qakbot Malware

QakBot 2021-06-10 · ZAYOTEM · Abdulkadir Binan, Emrah Sarıdağ, Emre Doğan, İlker Verimoğlu, Kaan Binen

QakBot Technical Analysis Report

QakBot 2021-06-08 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

From QBot...with REvil Ransomware: Initial Attack Exposure of JBS

QakBot REvil 2021-06-02 · Bleeping Computer · Lawrence Abrams

FUJIFILM shuts down network after suspected ransomware attack

QakBot 2021-05-26 · DeepInstinct · Ron Ben Yizhak

A Deep Dive into Packing Software CryptOne

Cobalt Strike Dridex Emotet Gozi ISFB Mailto QakBot SmokeLoader WastedLocker Zloader 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 2021-05-04 · Seguranca Informatica · Pedro Tavares

A taste of the latest release of QakBot

QakBot 2021-04-30 · MADRID Labs · Odin Bernstein

Qbot: Analyzing PHP Proxy Scripts from Compromised Web Server

QakBot 2021-04-28 · Reversing Labs · Karlo Zanki

Spotting malicious Excel4 macros

QakBot 2021-04-28 · IBM · David Bisson

QBot Malware Spotted Using Windows Defender Antivirus Lure

QakBot 2021-04-19 · Twitter (@_alex_il_) · Alex Ilgayev

Tweet on QakBot's additional decryption mechanism

QakBot 2021-04-15 · AT&T · Dax Morrow, Ofer Caspi

The rise of QakBot

QakBot 2021-04-13 · Silent Push · Martijn Grooten

Malicious infrastructure as a service

IcedID PhotoLoader QakBot 2021-04-12 · PTSecurity · PTSecurity

PaaS, or how hackers evade antivirus software

Amadey Bunitu Cerber Dridex ISFB KPOT Stealer Mailto Nemty Phobos Pony Predator The Thief QakBot Raccoon RTM SmokeLoader Zloader 2021-04-12 · Twitter (@elisalem9) · Eli Salem

Tweets on QakBot

QakBot 2021-04-06 · Intel 471 · Intel 471

EtterSilent: the underground’s new favorite maldoc builder

BazarBackdoor ISFB QakBot TrickBot 2021-03-31 · Red Canary · Red Canary

2021 Threat Detection Report

Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 2021-03-26 · Trend Micro · Trend

Micro

Alleged Members of Egregor Ransomware Cartel Arrested

Egregor QakBot 2021-03-18 · VinCSS · m4n0w4r, Tran Trung Kien

[RE021] Qakbot analysis – Dangerous malware has been around for more than a decade

QakBot 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 2021-02-24 · IBM · IBM SECURITY X-FORCE

X-Force Threat Intelligence Index 2021

Emotet QakBot Ramnit REvil 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 2021-02-15 · Twitter (@TheDFIRReport) · The DFIR Report

Tweet on Qakbot post infection discovery activity

QakBot 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 2021-01-19 · Medium elis531989 · Eli Salem

Funtastic Packers And Where To Find Them

Get2 IcedID QakBot 2021-01-19 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Emotet Infection Traffic

Emotet GootKit IcedID QakBot TrickBot 2021-01-06 · FBI · FBI

PIN Number 20210106-001: Egregor Ransomware Targets Businesses Worldwide, Attempting to Extort Businesses by Publicly Releasing Exfiltrated Data

Egregor QakBot 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD LAGOON

QakBot MALLARD SPIDER 2020-12-15 · Hornetsecurity · Hornetsecurity Security Lab

QakBot reducing its on disk artifacts

Egregor PwndLocker QakBot 2020-12-12 · Medium 0xthreatintel · 0xthreatintel

Reversing QakBot [TLP: White]

QakBot 2020-12-09 · InfoSec Handlers Diary Blog · Brad Duncan

Recent Qakbot (Qbot) activity

Cobalt Strike QakBot 2020-12-09 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations (SLIDES)

Cobalt Strike DoppelPaymer QakBot REvil 2020-12-03 · Recorded Future · Insikt Group®

Egregor Ransomware, Used in a String of High-Profile Attacks, Shows Connections to QakBot

Egregor QakBot 2020-12-02 · Red Canary · twitter (@redcanary)

Tweet on increased #Qbot activity delivering Cobalt Strike & #Egregor ransomware

Cobalt Strike Egregor QakBot 2020-12-01 · Group-IB · Group-IB, Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Egregor ransomware: The legacy of Maze lives on

Egregor QakBot 2020-11-30 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations

Cobalt Strike DoppelPaymer MimiKatz QakBot REvil 2020-11-27 · Fiducia & GAD IT AG · Frank Boldewin

When ransomware hits an ATM giant - The Diebold Nixdorf case dissected

PwndLocker QakBot 2020-11-26 · Cybereason · Cybereason Nocturnus, Lior Rochberger

Cybereason vs. Egregor Ransomware

Cobalt Strike Egregor IcedID ISFB QakBot 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 2020-11-20 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

The Locking Egregor

Egregor QakBot 2020-11-12 · Intrinsec · Jean Bichet

Egregor – Prolock: Fraternal Twins ?

Egregor PwndLocker QakBot 2020-10-29 · CERT-FR · CERT-FR

LE MALWARE-AS-A-SERVICE EMOTET

Dridex Emotet ISFB QakBot 2020-10-14 · CrowdStrike · The Falcon Complete Team

Duck Hunting with Falcon Complete: Remediating a Fowl Banking Trojan, Part 3

QakBot 2020-10-07 · CrowdStrike · The Falcon Complete Team

Duck Hunting with Falcon Complete: Analyzing a Fowl Banking Trojan, Part 2

QakBot Zloader 2020-10-01 · CrowdStrike · Dylan Barker, Quinten Bowen, Ryan Campbell

Duck Hunting with Falcon Complete: Analyzing a Fowl Banking Trojan, Part 1

QakBot MALLARD SPIDER 2020-09-29 · Microsoft · Microsoft

Microsoft Digital Defense Report

Emotet IcedID Mailto Maze QakBot REvil RobinHood TrickBot 2020-09-29 · PWC UK · Andy Auld

What's behind the increase in ransomware attacks this year?

DarkSide Avaddon Clop Conti DoppelPaymer Dridex Emotet FriedEx Mailto PwndLocker QakBot REvil Ryuk

SMAUG SunCrypt TrickBot WastedLocker 2020-09-10 · Group-IB · Oleg Skulkin, Semyon Rogachev

Lock Like a Pro: Dive in Recent ProLock's Big Game Hunting

PwndLocker QakBot 2020-09-10 · QuoSec GmbH · Quosec Blog

grap: Automating QakBot strings decryption

QakBot 2020-09-04 · QuoSec GmbH · Quosec Blog

Navigating QakBot samples with grap

QakBot 2020-08-27 · Checkpoint · Alex Ilgayev

An Old Bot’s Nasty New Tricks: Exploring Qbot’s Latest Attack Methods

QakBot 2020-08-20 · Morphisec · Arnold Osipov

QakBot (QBot) Maldoc Campaign Introduces Two New Techniques into Its Arsenal

QakBot 2020-07-15 · N1ght-W0lf Blog · Abdallah Elshinbary

Deep Analysis of QBot Banking Trojan

QakBot 2020-06-24 · Morphisec · Arnold Osipov

Obfuscated VBScript Drops Zloader, Ursnif, Qakbot, Dridex

Dridex ISFB QakBot Zloader 2020-06-21 · Malware and Stuff · Andreas Klopsch

UpnP – Messing up Security since years

QakBot 2020-06-16 · Hornetsecurity · Security Lab

QakBot malspam leading to ProLock: Nothing personal just business

PwndLocker QakBot 2020-06-11 · F5 Labs · Doron Voolf

Qbot Banking Trojan Still Up to Its Old Tricks

QakBot 2020-05-05 · Malware and Stuff · Andreas Klopsch

An old enemy – Diving into QBot part 3

QakBot 2020-03-30 · Malware and Stuff · Andreas Klopsch

An old enemy – Diving into QBot part 1

QakBot 2020-03-04 · CrowdStrike · CrowdStrike

2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 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 2020-02-19 · FireEye · FireEye

M-Trends 2020

Cobalt Strike Grateful POS LockerGoga QakBot TrickBot 2020-02-13 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Qakbot Infections

QakBot 2020-02-10 · Malwarebytes · Adam Kujawa, Chris Boyd, David Ruiz, Jérôme Segura, Jovi Umawing, Nathan Collier, Pieter Arntz, Thomas Reed, Wendy Zamora

2020 State of Malware Report

magecart Emotet QakBot REvil Ryuk TrickBot WannaCryptor 2020-01-03 · Youtube (BSides Belfast) · Jorge Rodriguez, Nick Summerlin

Demystifying QBot Banking Trojan

QakBot 2020-01-01 · Secureworks · SecureWorks

GOLD LAGOON

QakBot 2020-01-01 · University of Malta · Steve Borg

Memory Forensics of Qakbot

QakBot 2019-12-07 · Secureworks · Keith Jarvis, Kevin O'Reilly

End-to-end Botnet Monitoring... Botconf 2019

Emotet ISFB QakBot 2019-11-12 · Hatching.io · Markel Picado

Reversing Qakbot

QakBot 2019-06-03 · Varonis · Dolev Taler, Eric Saraga

Varonis Exposes Global Cyber Campaign: C2 Server Actively Compromising Thousands of Victims

QakBot 2019-05-02 · Cisco Talos · Ashlee Benge, Nick Randolph

Qakbot levels up with new obfuscation techniques

QakBot 2018-07-29 · Vitali Kremez Blog · Vitali Kremez

Let's Learn: In-Depth Reversing of Qakbot "qbot" Banker Part 1

QakBot 2018-03-18 · YouTube (BSidesBudapest - IT Security Conference) · Sandor Nemes

Spying on botnets

Corebot QakBot 2017-11-06 · Microsoft · Microsoft Defender ATP Research Team

Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks

Emotet QakBot 2017-06-02 · SecurityIntelligence · Kevin Zuk, Limor Kessem, Matan Meir, Mike Oppenheim

QakBot Banking Trojan Causes Massive Active Directory Lockouts

QakBot 2017-05-23 · ThreatVector · Cylance Threat Research Team

Quakbot

QakBot 2016-08-01 · Intel Security · Guilherme Venere, Mark Olea, Sanchit Karve

DIVING INTO PINKSLIPBOT'S LATEST CAMPAIGN

QakBot 2016-04-28 · Cisco Talos · Ben Baker

Research Spotlight: The Resurgence of Qbot

QakBot 2016-02-24 · Johannes Bader Blog · Johannes Bader

The DGA of Qakbot.T

QakBot 2016-01-01 · BAE Systems · BAE Systems

The Return of Qbot

QakBot 2012-01-01 · Symantec · Nicolas Falliere

W32.Qakbot in Detail

QakBot 2011-12-11 · Open Security Research · Michael G. Spohn.

Intro. To Reversing - W32Pinkslipbot

QakBot 2011-05-25 · Contagio Dump · Mila Parkour

W32.Qakbot aka W32/Pinkslipbot or infostealer worm

QakBot 2010-10-25 · RSA · RSA FraudAction Research Labs

Businesses Beware: Qakbot Spreads like a Worm, Stings like a Trojan

QakBot 2010-05-11 · Symantec · Shunichi Imano

Qakbot, Data Thief Unmasked: Part I

QakBot 2010-04-22 · Symantec · Patrick Fitzgerald

Qakbot Steals 2GB of Confidential Data per Week

QakBot 2009-12-22 · Symantec · John McDonald, Masaki Suenaga, Takayoshi Nakayama

Qakbot, Data Thief Unmasked: Part II

QakBot 2009-05-07 · Symantec · Angela Thigpen, Eric Chien

W32.Qakbot

QakBot

▶ [TLP:WHITE] win_qakbot_auto (20251219 | Detects win.qakbot.)
