More_eggs (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:41:50 UTC

More_eggs

aka: SpicyOmelette, SKID

Actor(s): Cobalt, FIN6, VENOM SPIDER

More_eggs is a JavaScript backdoor used by the Cobalt group. It attempts to connect to its C&C server and retrieve tasks to carry out, some of which are:
- d&exec = download and execute PE file
- gtfo = delete files/startup entries and terminate
- more_eggs = download additional/new scripts
- more_onion = run new script and terminate current script
- more_power = run command shell commands

References

2025-05-17 · Denwp Research ·
More_Eggs? A Venom Spider Backdoor Targeting HR
More_eggs

2025-05-02 · Arctic Wolf · Arctic Wolf Labs Team
Venom Spider Uses Server-Side Polymorphism to Weave a Web Around Victims
More_eggs

2024-12-02 · The DFIR Report · The DFIR Report
The Curious Case of an Egg-Cellent Resume
More_eggs Pyramid Cobalt Strike

2024-06-10 · The Hacker News · Ravie Lakshmanan
More_eggs Malware Disguised as Resumes Targets Recruiters in Phishing Attack
More_eggs

2023-12-12 · Proofpoint · Kelsey Merriman, Selena Larson, Xavier Chambrier
Security Brief: TA4557 Targets Recruiters Directly via Email
More_eggs FIN6

2023-04-20 · Securonix · Den Iyzvyk, Oleg Kolesnikov, Tim Peck
New OCX#HARVESTER Attack Campaign Leverages a Modernized More_eggs Suite to Target Victims

More_eggs

2023-03-10 · Security0wnage · Security0wnage

How Do You Like Dem Eggs? I like Mine Scrambled, Really Scrambled - A Look at Recent more_eggs Samples

More_eggs

2023-01-24 · eSentire · Joe Stewart, Keegan Keplinger

Unmasking Venom Spider

More_eggs TerraPreter TerraLoader VenomLNK

2022-08-25 · Expel · Andrew Jerry, Kyle Pellett

MORE_EGGS and Some LinkedIn Resumé Spearphishing

More_eggs

2022-04-21 · eSentire · eSentire Threat Response Unit (TRU)

Hackers Spearphish Corporate Hiring Managers with Poisoned Resumes, Infecting Them with the More_Eggs Malware, Warns eSentire

More_eggs TerraLoader VenomLNK

2021-04-05 · eSentire · eSentire

Hackers Spearphish Professionals on LinkedIn with Fake Job Offers, Infecting them with Malware, Warns eSentire

More_eggs TerraPreter TerraLoader VenomLNK

2020-09-03 · Twitter (@Arkbird_SOLG) · Arkbird

Tweet on development in more_eggs

More_eggs

2020-07-20 · QuoIntelligence

Golden Chickens: Evolution Oof the MaaS

More_eggs TerraLoader TerraStealer VenomLNK

2020-07-10 · Github (eset) · Matías Porolli

Evilnum — Indicators of Compromise

EVILNUM More_eggs EVILNUM TerraStealer

2020-07-09 · ESET Research · Matías Porolli

More evil: A deep look at Evilnum and its toolset

EVILNUM More_eggs EVILNUM TerraPreter TerraStealer TerraTV Evilnum

2020-06-04 · · Chianxin Virus Response Center

脚本系贼寇之风兴起，买卖体系堪比勒索软件

EVILNUM More_eggs

2020-04-07 · SecurityIntelligence · Ole Villadsen

ITG08 (aka FIN6) Partners With TrickBot Gang, Uses Anchor Framework

More_eggs Anchor TrickBot

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

2020-02-13 · Qianxin · Qi Anxin Threat Intelligence Center

APT Report 2019

Chrysaor Exodus Dacls VPNFilter DNSRat Griffon KopiLuwak More_eggs SQLRat AppleJeus BONDUPDATER Agent.BTZ Anchor AndroMut AppleJeus BOOSTWRITE Brambul Carbanak Cobalt Strike Dacls DistTrack DNSpionage Dtrack ELECTRICFISH FlawedAmmyy FlawedGrace Get2 Grateful POS HOPLIGHT Imminent Monitor RAT jason Joanap KerrDown KEYMARBLE Lambert LightNeuron LoJax MiniDuke PolyglotDuke PowerRatankba Rising Sun SDBbot ServHelper Snatch Stuxnet TinyMet tRat TrickBot Volgmer X-Agent Zebrocy

2020-01-01 · Secureworks · SecureWorks

GOLD KINGSWOOD

More_eggs ATMSpitter Cobalt Strike CobInt MimiKatz

2020-01-01 · Secureworks · SecureWorks

GOLD KINGSWOOD

More_eggs ATMSpitter Cobalt Strike CobInt MimiKatz Cobalt

2019-08-29 · Security Intelligence · Joey Victorino, Kevin Henson, Melissa Frydrych, Ole Villadsen

More_eggs, Anyone? Threat Actor ITG08 Strikes Again

More_eggs FIN6

2019-06-04 · Bitdefender · Bitdefender

An APT Blueprint: Gaining New Visibility into Financial Threats

More_eggs Cobalt Strike

2019-02-21 · Proofpoint · Proofpoint Threat Insight Team

Fake Jobs: Campaigns Delivering More_eggs Backdoor via Fake Job Offers

More_eggs FIN6

2018-10-17 · MITRE ATT&CK · MITRE
Software Description: More_eggs
More_eggs

2018-10-08 · Morphisec · Michael Gorelik
Cobalt Group 2.0
More_eggs

2018-09-27 · Secureworks · Counter Threat Unit ResearchTeam
Cybercriminals Increasingly Trying to Ensnare the Big Financial Fish
More_eggs Cobalt

2018-08-30 · NetScout · ASERT Team
Double the Infection, Double the Fun
More_eggs CobInt

2018-07-31 · Cisco Talos · Vanja Svajcer
Multiple Cobalt Personality Disorder
More_eggs

2018-03-02 · Reaqta · Reaqta
Spear-phishing campaign leveraging on MSXSL
More_eggs

2017-11-20 · Trend Micro · Fyodor Yarochkin, Lenart Bermejo, Ronnie Giagone
Cobalt Strikes Again: Spam Runs Use Macros and CVE-2017-8759 Exploit Against Russian Banks
More_eggs Cobalt

2017-08-07 · Trend Micro · Fyodor Yarochkin, Lenart Bermejo, Ronnie Giagone, Rubio Wu
Backdoor-carrying Emails Set Sights on Russian-speaking Businesses
More_eggs

There is no Yara-Signature yet.
