TEARDROP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:03:15 UTC

TEARDROP is a memory only dropper that runs as a service, spawns a thread and reads from the file “gracious_truth.jpg”, which likely has a fake JPG header. Next it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm and manually loads into memory an embedded payload using a custom PE-like file format. TEARDROP does not have code overlap with any previously seen malware. FireEye believe that this was used to execute a customized Cobalt Strike BEACON.

2022-07-31 · BushidoToken Blog ·
Space Invaders: Cyber Threats That Are Out Of This World
Poison Ivy Raindrop SUNBURST TEARDROP WastedLocker 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Solar Phoenix
SUNBURST TEARDROP UNC2452 2022-04-27 · Mandiant · Mandiant
Assembling the Russian Nesting Doll: UNC2452 Merged into APT29
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-07-13 · YouTube (Matt Soseman) · Matt Soseman
Solarwinds and SUNBURST attacks compromised my lab!
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-07-13 · Symantec · Threat Hunter Team
Attacks Against the Government Sector
Raindrop TEARDROP 2021-06-01 · SANS · Jake Williams, Kevin Haley
A Contrarian View on SolarWinds
Cobalt Strike Raindrop SUNBURST TEARDROP 2021-03-08 · Youtube (SANS Digital Forensics and Incident Response) · Adam Pennington, Jen Burns, Katie Nickels
STAR Webcast: Making sense of SolarWinds through the lens of MITRE ATT&CK(R)
Cobalt Strike SUNBURST TEARDROP 2021-03-04 · Microsoft · Andrea Lelli, Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC), Ramin Nafisi
GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM’s layered persistence
SUNBURST TEARDROP UNC2452 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 2021-02-16 · Accenture · Alexandrea Berninger
Hard lessons learned: Threat intel takeaways from the community response to Solarigate
SUNBURST TEARDROP 2021-02-09 · Securehat · Securehat
Extracting the Cobalt Strike Config from a TEARDROP Loader
Cobalt Strike TEARDROP 2021-02-08 · US-CERT · US-CERT

Malware Analysis Report (AR21-039B): MAR-10320115-1.v1 - TEARDROP

TEARDROP 2021-01-20 · Microsoft · Microsoft 365 Defender Research Team, Microsoft Cyber Defense Operations Center (CDOC), Microsoft Threat Intelligence Center (MSTIC)

Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop

Cobalt Strike SUNBURST TEARDROP 2021-01-18 · Symantec · Threat Hunter Team

Raindrop: New Malware Discovered in SolarWinds Investigation

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-01-12 · BrightTALK (FireEye) · Ben Read, John Hultquist

UNC2452: What We Know So Far

Cobalt Strike SUNBURST TEARDROP 2021-01-11 · SolarWinds · Sudhakar Ramakrishna

New Findings From Our Investigation of SUNBURST

Cobalt Strike SUNBURST TEARDROP 2021-01-04 · Twitter (@TheEnergyStory) · Dominik Reichel

Some small detail on compiler used for TEARDROP

TEARDROP 2021-01-01 · Symantec · Symantec Threat Hunter Team

Supply Chain Attacks:Cyber Criminals Target the Weakest Link

Cobalt Strike Raindrop SUNBURST TEARDROP 2020-12-28 · Microsoft · Microsoft 365 Defender Team

Using Microsoft 365 Defender to protect against Solorigate

SUNBURST TEARDROP 2020-12-24 · Twitter (@TheEnergyStory) · Dominik Reichel

Tweet on TEARDROP sample

TEARDROP 2020-12-23 · Palo Alto Networks Unit 42 · Unit 42

A Timeline Perspective of the SolarStorm Supply-Chain Attack

SUNBURST TEARDROP 2020-12-22 · Checkpoint · Check Point Research

SUNBURST, TEARDROP and the NetSec New Normal

SUNBURST TEARDROP 2020-12-22 · Medium mitre-attack · Adam Pennington, Matt Malone

Identifying UNC2452-Related Techniques for ATT&CK

SUNBURST TEARDROP UNC2452 2020-12-21 · Microsoft · MSRC Team

Solorigate Resource Center

SUNBURST TEARDROP 2020-12-21 · Fortinet · Udi Yavo

What We Have Learned So Far about the “Sunburst”/SolarWinds Hack

Cobalt Strike SUNBURST TEARDROP 2020-12-18 · Costin Raiu

Tweet from Costin Raiu about confirmed TEARDROP sample

TEARDROP 2020-12-18 · Microsoft · Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-12-14 · Symantec · Threat Hunter Team

Sunburst: Supply Chain Attack Targets SolarWinds Users

SUNBURST TEARDROP 2020-12-14 · Cisco Talos · Nick Biasini

Threat Advisory: SolarWinds supply chain attack

SUNBURST TEARDROP 2020-12-13 · FireEye · Alex Berry, Alex Pennino, Alyssa Rahman, Andrew Archer, Andrew Rector, Andrew Thompson, Barry Vengerik, Ben Read, Ben Withnell, Chris DiGiamo, Christopher Glyer, Dan Perez, Dileep Jallepalli, Doug Bienstock, Eric Scales, Evan Reese, Fred House, Glenn Edwards, Ian Ahl, Isif Ibrahima, Jay Smith, John Gorman, John Hultquist, Jon Leathery, Lennard Galang, Marcin Siedlarz, Matt Dunwoody, Matthew McWhirt, Michael Sikorski, Microsoft, Mike Burns, Nalani Fraiser, Nick Bennett, Nick Carr, Nick Hornick, Nick Richard, Nicole Oppenheim, Omer Baig, Ramin Nafisi, Sarah Jones, Scott

Runnels, Stephen Eckels, Steve Miller, Steve Stone, William Ballenthin

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-12-13 · Github (fireeye) · FireEye

SUNBURST Countermeasures

SUNBURST SUPERNOVA TEARDROP UNC2452 2020-01-22 · Thomas Barabosch

The malware analyst’s guide to PE timestamps

Azorult Gozi IcedID ISFB LOLSnif SUNBURST TEARDROP

There is no Yara-Signature yet.
