ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Threat Group Cards: A Threat Actor Encyclopedia

Tool: TEARDROP

Names	TEARDROP
Category	Malware
Type	Dropper
Description	(FireEye) Multiple SUNBURST samples have been recovered, delivering different payloads. In at least one instance the attackers deployed a previously unseen memory-only dropper we've dubbed TEARDROP to deploy Cobalt Strike BEACON.
Information	<https://us-cert.cisa.gov/ncas/alerts/aa20-352a> <http://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html> <https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html> <https://github.com/fireeye/sunburst_countermeasures> <https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html> <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/> <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/> <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/> <https://www.guidepointsecurity.com/analysis-of-the-solarwinds-supply-chain-attack/> <https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html> <https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/> <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-solarwinds-supply-chain-attack> <https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/> <https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/> <https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/> <https://www.cadosecurity.com/post/responding-to-solarigate> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data> <https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach> <https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sunburst-malware-and-solarwinds-supply-chain-compromise/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/how-a-device-to-cloud-architecture-defends-against-the-solarwinds-supply-chain-compromise/> <https://www.tripwire.com/state-of-security/vert/vert-alert-solar-winds-supply-chain-attack/> <https://blog.cyberint.com/solarwinds-supply-chain-attack> <https://blog.checkpoint.com/2020/12/21/best-practice-identifying-and-mitigating-the-impact-of-sunburst/> <https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/> <https://mp.weixin.qq.com/s/UqXC1vovKUu97569LkYm2Q> <https://blog.qualys.com/qualys-insights/2020/12/22/qualys-security-advisory-solarwinds-fireeye> <https://www.cyfirma.com/solarwinds-hack-sunburst-supernova-and-more/> <https://gist.github.com/SwitHak/8b59e740b187511caad1bf06caa44df1> <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b>
MITRE ATT&CK	<https://attack.mitre.org/software/S0560/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.teardrop>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool TEARDROP

Changed	Name	Country	Observed
APT groups			
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025

1 group listed (1 APT, 0 other, 0 unknown)

↑

Infrastructure and Security Department
Electronic Transactions Development Agency

Follow us on

Report incidents

+66 (0)2-123-1227

helpdesk@etda.or.th