Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:01:35 UTC

Tool: Bisonal

Names	Bisonal Korlia
Category	Malware
Type	Backdoor, Info stealer, Exfiltration, Downloader
Description	(Palo Alto) In early May, Unit 42 discovered an attack campaign against at least one defense company in Russia and one unidentified organization in South Korea delivering a variant of Bisonal malware. While not previously publicly documented, the variant has been in the wild since at least 2014. There are three primary differences between it and older Bisonal malware including a different cipher and encryption for C2 communication, and a large rewrite of the code for both network communication and maintaining persistence. To date, we have only collected 14 samples of this variant, indicating it may be sparingly used. The adversary behind these attacks lured the targets into launching the Microsoft Windows executable malware by masquerading it as a PDF file (using a fake PDF icon) and reusing publicly available data for the decoy PDF file's contents. Attacks using Bisonal have been blogged about in the past. In 2013, both COSEINC and FireEye revealed attacks using Bisonal against Japanese organizations. In October 2017, AhnLab published a report called "Operation Bitter Biscuit," an attack campaign against South Korea, Japan, India and Russia using Bisonal and its successors, Bioazih and Dexbia. We believe it is likely these tools are being used by one group of attackers.
Information	<https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea/> <https://camal.coseinc.com/publish/2013Bisonal.pdf> <https://www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf> <https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html> <https://securitykitten.github.io/2014/11/25/curious-korlia.html> <https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/>

MITRE ATT&CK	<https://attack.mitre.org/software/S0268/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.korlia>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:bisonal>

Last change to this tool card: 14 August 2020

Download this tool card in JSON format

All groups using tool Bisonal

Changed	Name	Country	Observed	
APT groups				
	Tonto Team, HartBeat, Karma Panda		2009-Apr 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c23db213-667e-48ca-ae9f-c19c503762ef