

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:14:41 UTC



## Tool: Minzen

Names	Minzen XXMM Wali ShadowWali ShadowWalker
Category	<a href="#">Malware</a>
Type	<a href="#">Loader</a>
Description	( <a href="#">Palo Alto</a> ) Minzen is a modular malware that has both 32-bit and 64-bit components in its resource section or configuration data in its body.
Information	< <a href="https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/">https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/</a> > < <a href="http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/">http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/</a> > < <a href="https://jsac.jpCERT.or.jp/archive/2019/pdf/JSAC2019_8_nakatsuru_en.pdf">https://jsac.jpCERT.or.jp/archive/2019/pdf/JSAC2019_8_nakatsuru_en.pdf</a> > < <a href="https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses">https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.xmmm">https://malpedia.caad.fkie.fraunhofer.de/details/win.xmmm</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:Minzen">https://otx.alienvault.com/browse/pulses?q=tag:Minzen</a> >

Last change to this tool card: 14 May 2020

Download this tool card in [JSON](#) format

### All groups using tool Minzen

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Bronze Butler, Tick, RedBaldNight, Stalker Panda</a>		2006-Apr 2021 

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



---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=6556f750-eaad-42bc-ba0f-b9895199f159>