Threat Group Cards: A Threat Actor Encyclopedia

Tool: Protux

Names	Protux
Category	Malware
Type	Backdoor
Description	(Trend Micro) Protux, a known backdoor, is executed by abusing the rundll32 dynamic-link library (DLL). It tests the host's network, retrieves the C&C server from another blog, and uses the RSA algorithm to generate the session key and send information to the C&C server.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:protux>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Protux

Changed	Name	Country	Observed	
APT groups				
	Blackgear		2018-Jul 2018	

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