Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:20:29 UTC

Tool: XPCTRA

Names	XPCTRA Expectra
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer
Description	(SANS) • The infection vector (malspam) links to a supposed PDF invoice, which actually leads the victim to download an executable file (dropper); • Once executed, the dropper downloads a ".zip" file, unzips and executes the malware payload; • It then begins a series of actions, including: o Persists itself into the OS, in order to survive system reboot; o Changes Firewall policies to allow the malware to communicate unrestrictedly with the Internet; o Instantiates "Fliddler", an HTTP Proxy that is used to monitor and intercept user access to the financial institution o Installs the Fiddler root certificate to prevent the user from receiving digital certificate errors; o Points Internet Browsers settings to the local proxy (Fiddler); o Monitors and captures user credentials while accessing the websites of 2 major Brazilian banks and other financia institutions; o Stolen credentials are sent to criminals through an unencrypted C&C channel; o Establishes an encrypted channel to allow the victim's system to be controlled by the attackers (RAT); o Monitors and captures user credentials while accessing email services like Microsoft Live, Terra, IG and Hotmail These accesses are used to spread the malware further; After posting EngineBox malware analysis last month, through community feedback, I came to know that the threa embedded a framework called QuasarRAT developed in C#. The goal of this framework is to provide a tool for rem access and management of Windows computers— hence the name, RAT (Remote Access Tool).
Information	<https://isc.sans.edu/forums/diary/XPCTRA+Malware+Steals+Banking+and+Digital+Wallet+Users+Credentials/2
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.xpctra>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:xpctra>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool XPCTRA

Changed	Name	Country	Observed
Unknown groups			

	[Interesting malware not linked to an actor yet]			

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