Free Darktrack RAT Has the Potential of Being the Best RAT on the Market

news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml

Catalin Cimpanu September 11, 2016

A remote access trojan (RAT) developed and provided for free by a malware coder named Luckyduck is actually as good as other top-shelf commercial RATs available today.

This freemium distribution model is strange on today's malware scene where all powerful toolkits are available for a price on underground hacking forums or Dark Web marketplaces, especially if they're actually any good.

Free RATs are often incomplete, easily detected by antivirus engines, and often backdoored by their creators.

That's why, when a security researcher that goes by the name of MalwareHunterTeam came across a Darktrack sample at the end of August, things just didn't add up.

Darktrack as good as commercial RATs

The RAT was full of powerful features, usually found in commercial RATs. But when MalwareHunterTeam tracked down the RAT's homepage, he discovered that Darktrack's creator was offering it for free, and pledging to do so forever.

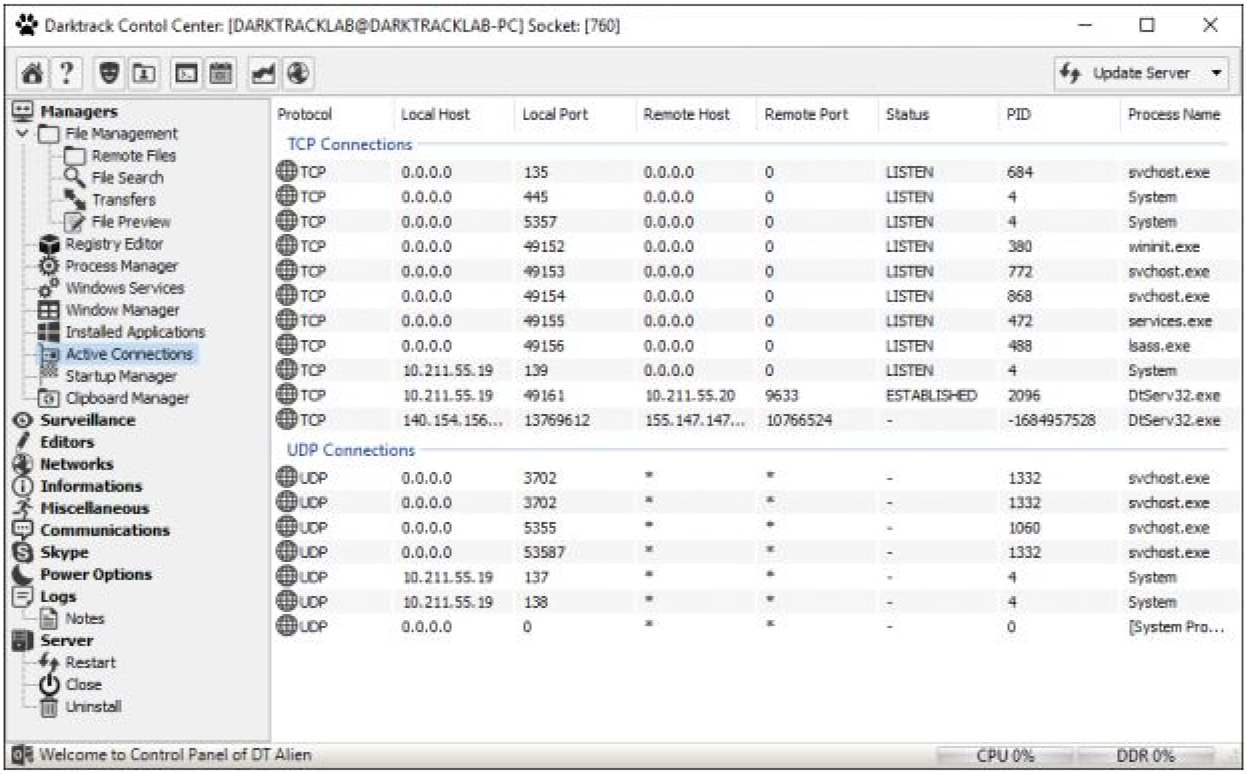
MalwareHunterTeam had come across Darktrack version 4.0. In the meantime, after the researcher's tip-off, Softpedia has been keeping an eye out for Darktrack mentions online, trying to see how this RAT evolved.

As it turns out, on the same day that MalwareHunterTeam discovered version 4.0, Luckyduck opened a thread on one of the largest underground hacking forums, teasing an upcoming version called Darktrack Alien+ 4.1.

"The previous [4.0] version was also at least as good as the current 'best selling' RATs," MalwareHunterTeam told Softpedia. "If the new version will be even better, and still free, don't think there is any reason to buy a paid RAT."

Malware author doing business on the public Internet

Answering questions from other forum users, Luckyduck said that a new and improved version was very close to its release. On September 4, Luckyduck uploaded a video on YouTube (now delisted, check udpate at the end of the article) showing Darktrack Alien+ 4.1 during early tests.



Darktrack Contol Center: [DARKTRACKLAB@DARKTRACKLAB-PC] Socket: [760]

Protocol	Local Host	Local Port	Remote Host	Remote Port	Status	PID	Process Name
TCP Connections							
TCP	0.0.0.0	135	0.0.0.0	0	LISTEN	684	svchost.exe
TCP	0.0.0.0	445	0.0.0.0	0	LISTEN	4	System
TCP	0.0.0.0	5357	0.0.0.0	0	LISTEN	4	System
TCP	0.0.0.0	49152	0.0.0.0	0	LISTEN	380	wininit.exe
TCP	0.0.0.0	49153	0.0.0.0	0	LISTEN	772	svchost.exe
TCP	0.0.0.0	49154	0.0.0.0	0	LISTEN	868	svchost.exe
TCP	0.0.0.0	49155	0.0.0.0	0	LISTEN	472	services.exe
TCP	0.0.0.0	49156	0.0.0.0	0	LISTEN	488	lsass.exe
TCP	10.211.55.19	139	0.0.0.0	0	LISTEN	4	System
TCP	10.211.55.19	49161	10.211.55.20	9633	ESTABLISHED	2096	DtServ32.exe
TCP	140.154.156...	13769612	155.147.147...	10766524	-	-1684957528	DtServ32.exe
UDP Connections							
UDP	0.0.0.0	3702	*	*	-	1332	svchost.exe
UDP	0.0.0.0	3702	*	*	-	1332	svchost.exe
UDP	0.0.0.0	5355	*	*	-	1060	svchost.exe
UDP	0.0.0.0	53587	*	*	-	1332	svchost.exe
UDP	10.211.55.19	137	*	*	-	4	System
UDP	10.211.55.19	138	*	*	-	4	System
UDP	0.0.0.0	0	*	*	-	0	[System Pro...

Welcome to Control Panel of DT Alien

Darktrack RAT GUI

The malware coder also runs a dedicated website for Darktrack on the public Internet. He also runs a support topic, Facebook, Twitter, and Google+ pages, and brazenly lists his Skype ID. His YouTube channel also features many Darktrack tutorials.

Domain whois information returns the details of a man named Ekrem Karatas from Istanbul, Turkey. This may be a fake identity, so we wouldn't put too much trust into this information. Performing a strict Google search for this person's Gmail address returns only results associated with the Darktrack domain.

Darktrack comes with a keylogger, DDoS module, more

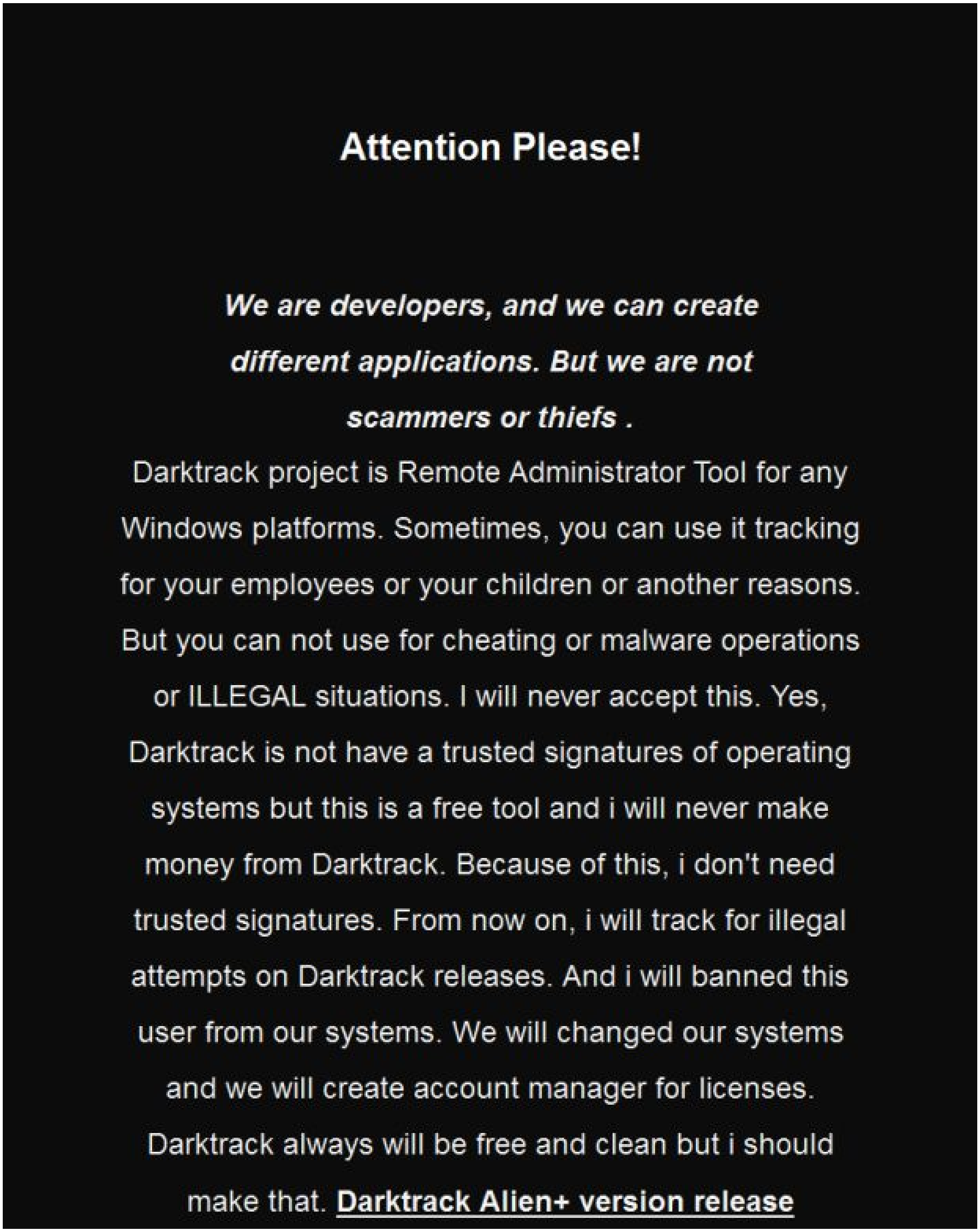
According to his forum post, this free RAT is choke-full with all types of features you've previously seen in commercial RATs such as Orcus or JBifrost (Adwind).

Here is just a short list of advertised features. You can read the full list at the end of this article. According to its forum post and official website, Darktrack comes with the ability to connect to remote computers and access their filesystem, the ability to spy via webcams, log keystrokes, dump passwords, and perform network stress tests (DDoS attacks).

There is also a port scanner, an interface to interact with the victim's task scheduler, a system monitoring tool, a clipboard data logger, a startup program manager, a hosts file editor, a Windows Registry editor, the ability to execute commands on infected PCs, and interact with local processes and services.

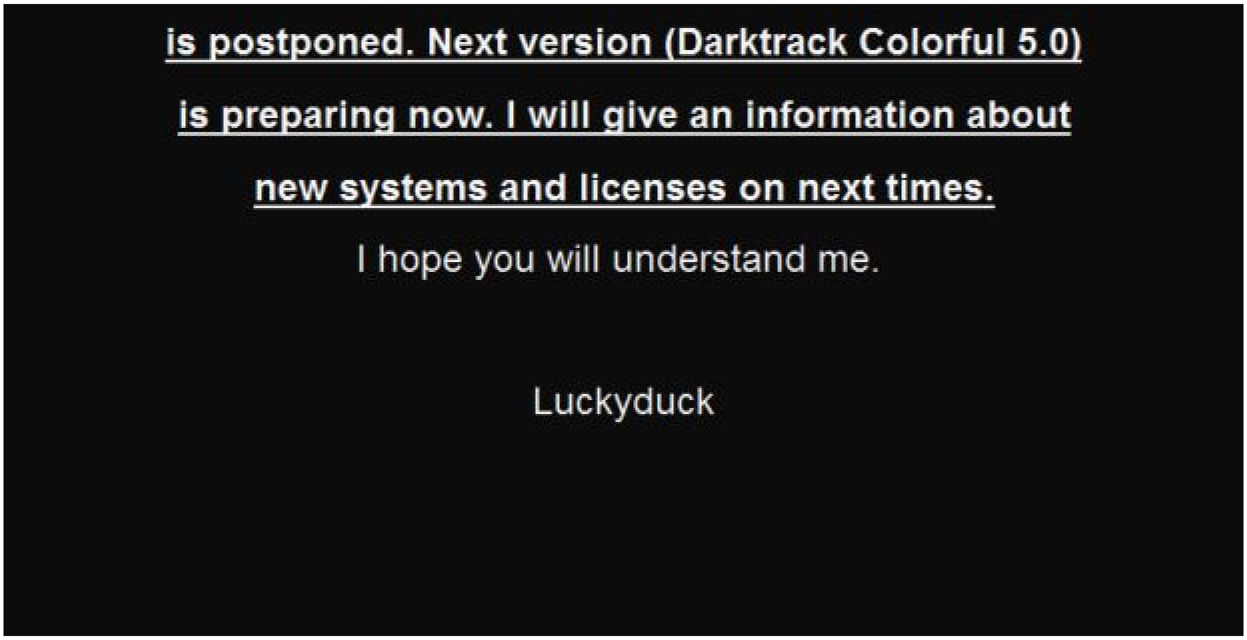
Almost everything you find in commercial RATs is included. "Maybe a good plugin system is what could be a reason for buying a commercial RAT if Darktrack does not have one," MalwareHunterTeam also added. "But I think average skids don't care."

UPDATE [September 14, 2016]: Following our article and the attention the RAT received from security researchers, Luckyduck shut down the Draktrack website and published the following message.



Attention Please!

We are developers, and we can create different applications. But we are not scammers or thiefs .
Darktrack project is Remote Administrator Tool for any Windows platforms. Sometimes, you can use it tracking for your employees or your children or another reasons. But you can not use for cheating or malware operations or ILLEGAL situations. I will never accept this. Yes, Darktrack is not have a trusted signatures of operating systems but this is a free tool and i will never make money from Darktrack. Because of this, i don't need trusted signatures. From now on, i will track for illegal attempts on Darktrack releases. And i will banned this user from our systems. We will changed our systems and we will create account manager for licenses. Darktrack always will be free and clean but i should make that. **Darktrack Alien+ version release**



is postponed. Next version (Darktrack Colorful 5.0)
is preparing now. I will give an information about
new systems and licenses on next times.
I hope you will understand me.

Luckyduck

Message on Darktrack website after it shut down