Blackremote: Money Money Money – A Swedish Actor Peddles an Expensive New RAT

unit42.paloaltonetworks.com/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/

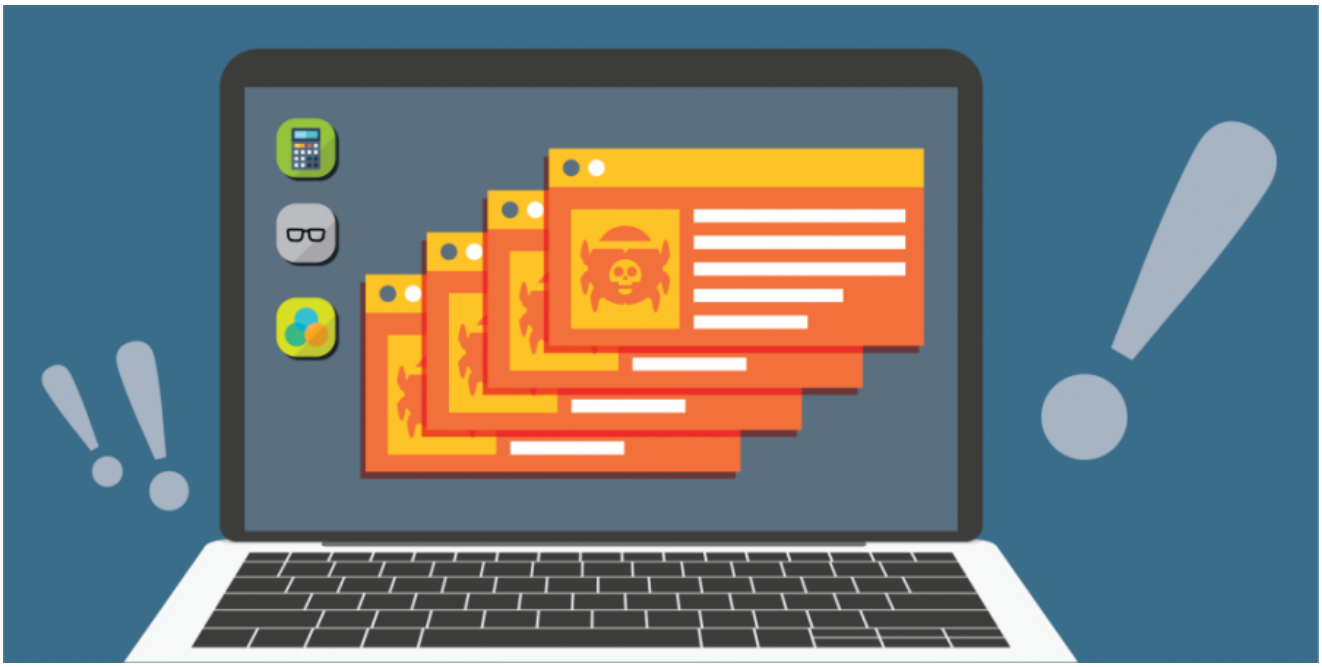
Unit 42 October 15, 2019

By Unit 42

October 15, 2019 at 6:00 AM

Category: Malware, Unit 42

Tags: Blackremote, commodity, Cybercrime, RAT



This post is also available in: 日本語 (Japanese)

Executive Summary

While researching prevalent commodity Remote Access Tools (RATs), Unit 42 researchers discovered a new, undocumented RAT in September, which had almost 50 samples observed in more than 2,200 attack sessions within the first month it was sold. In this report, we document the RAT manager/builder, client malware, and profile the Swedish actor behind this together with his promotion and sale of his malware. We also document this RAT already being used in malicious attacks in the wild.

Promoting his RAT

During the first week of September 2019, the actor started promoting his new RAT on several underground forums (Figure 1), using the handles Speccy and Rafiki. The succinct posts shared a link to his sales site blackremote[.]pro, and his discord handle Speccy#0100.

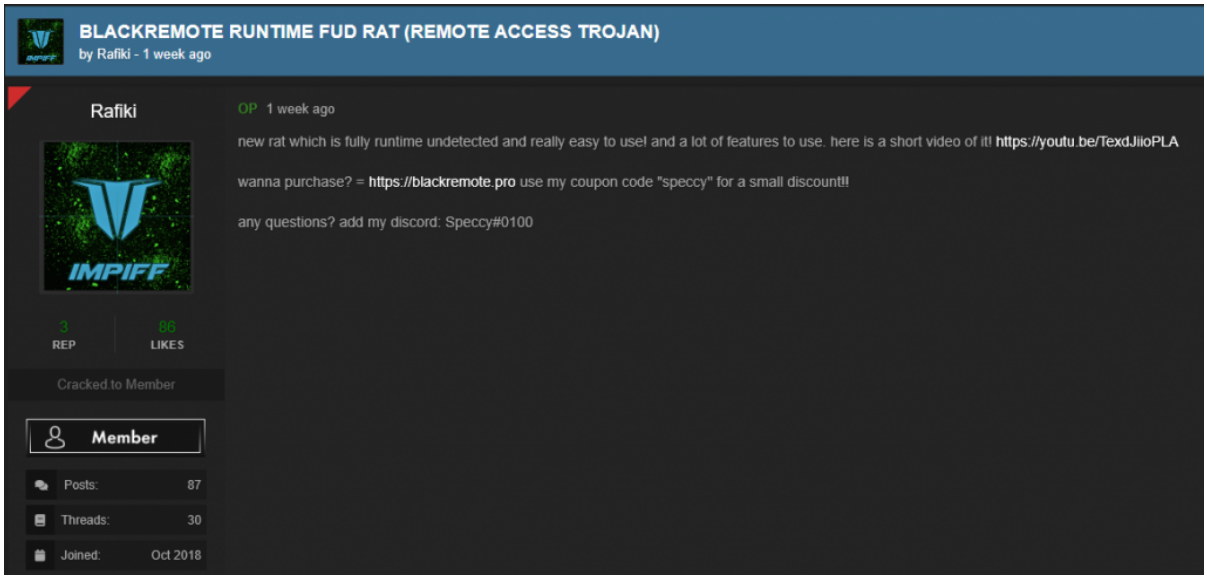


Figure 1. RAT promoted on forums

During the same week, he posted a YouTube video (Figure 2), with instructions for setting up his RAT.

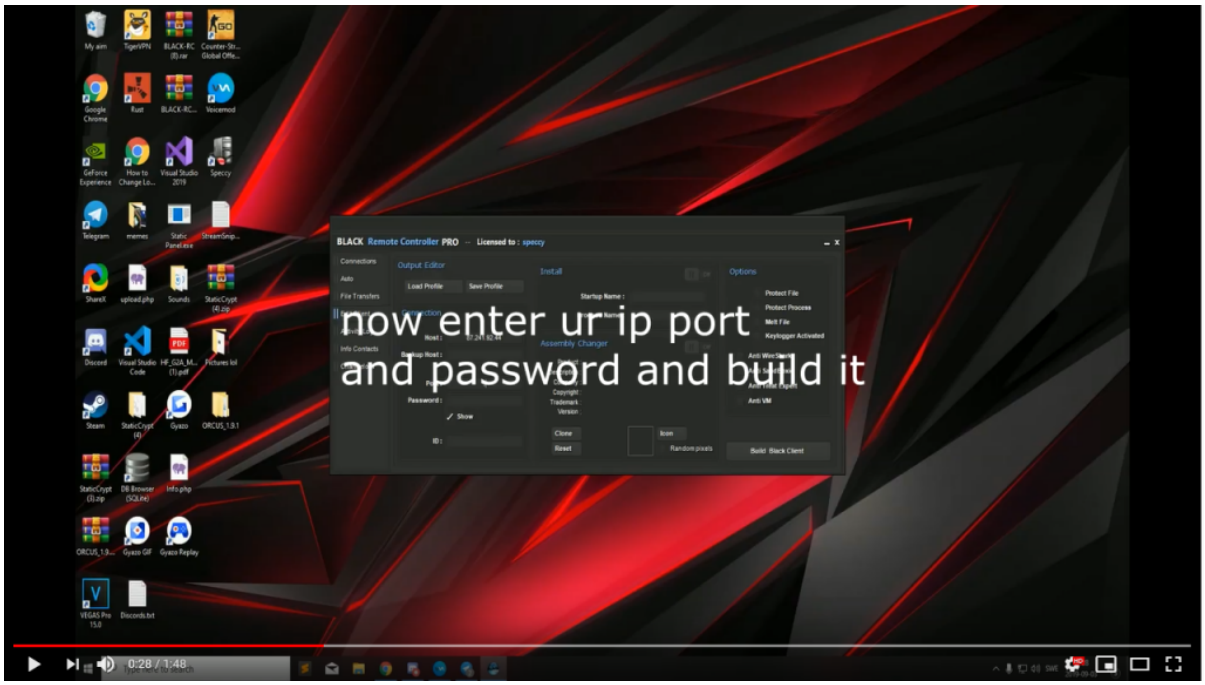


Figure 2. YouTube "how-to" video

The YouTube description (Figure 3) included a link to his personal site speccy[.]dev. It also included the claim "*this rat is fully runtime undetected*" and a link to "*purchase FUD crypter.*" There is no legitimate reason for this software to need to be "undetectable" or "crypted." Rather, such efforts are intended to prevent detection by antimalware software.

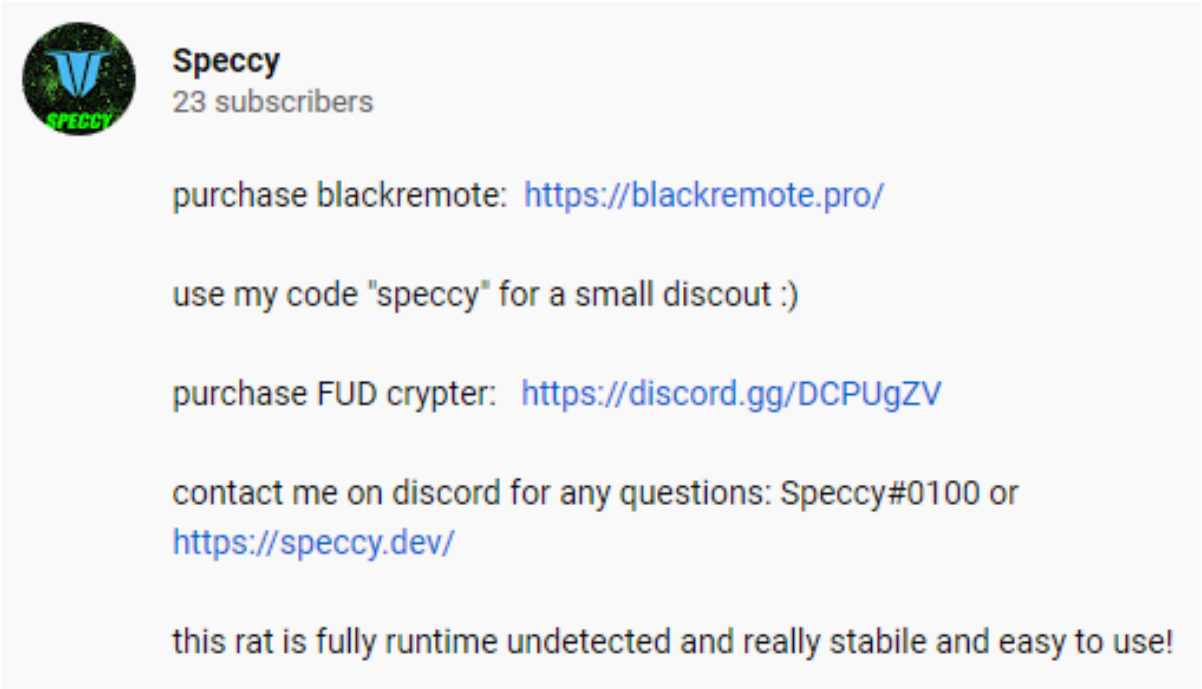


Figure 3. YouTube description

blackremote[.]pro

The sales site for Blackremote RAT, blackremote[.]pro (Figure 4), was registered on August 19, 2019.

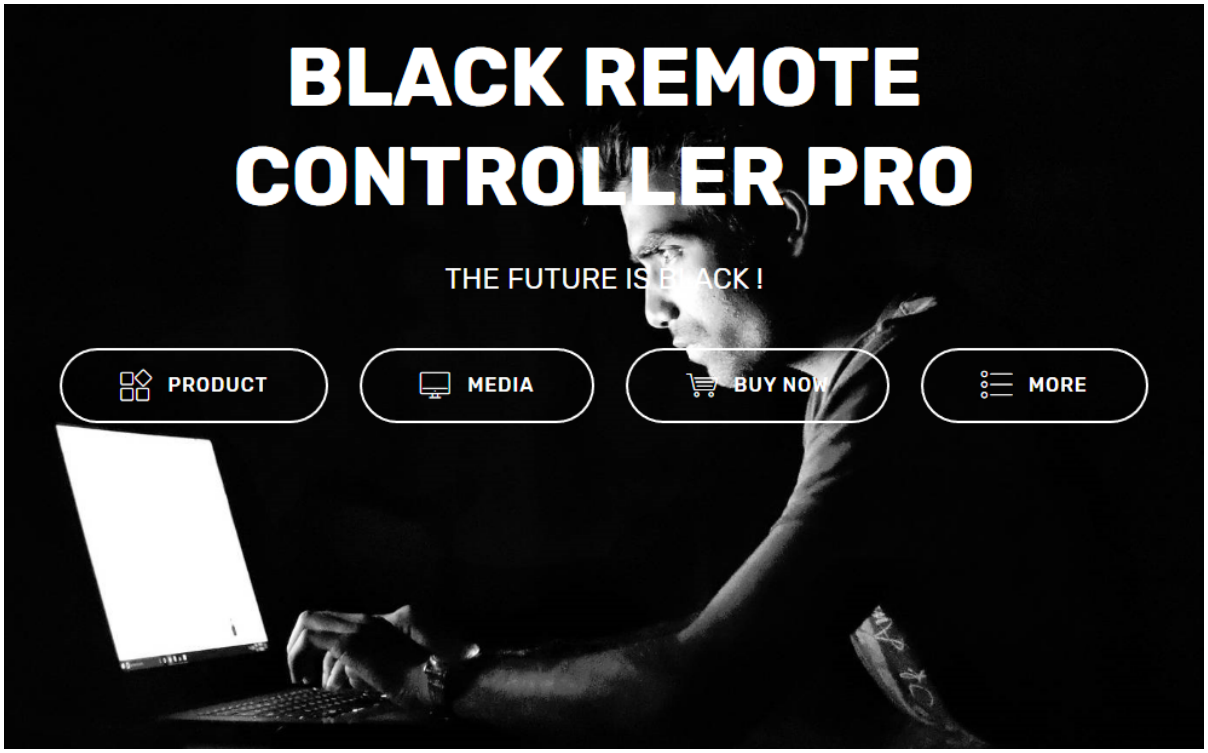


Figure 4. blackremote[.]pro

Speccy describes his RAT:

"Black Remote Controller PRO is a powerful and full featured systems remote admnistration suite. It will give you full access and control over a remote machine through a countless number of features, giving you the ability to monitor, access or manipulate every activity and data remotely, just like you are in front of it!"

As is typical with other malicious RATs promoted at the same underground forums, Speccy claims legitimate purpose:

"This tool is ideal for everyone who necessitate to access, monitor or operate remotely on a given system for a wide and various range of needs, administration professionals, parental control, forensics, sourveillance [sic]*, remote assistance. Black will become for you an incredible tool to achieve everything remotely."*

However, the previously mentioned claims of being "undetectable" and references to crypting, together with features such as "Password Recovery" and his "Fun Features" (Figure 5) advertising ("*We all know sometimes things may get boring, expecially* [sic] *in professional and tech environment*" … "*Black Remote Controller may become also a funny tool for jokes, why not?*") are hardly in keeping with a tool designed for legitimate purpose.

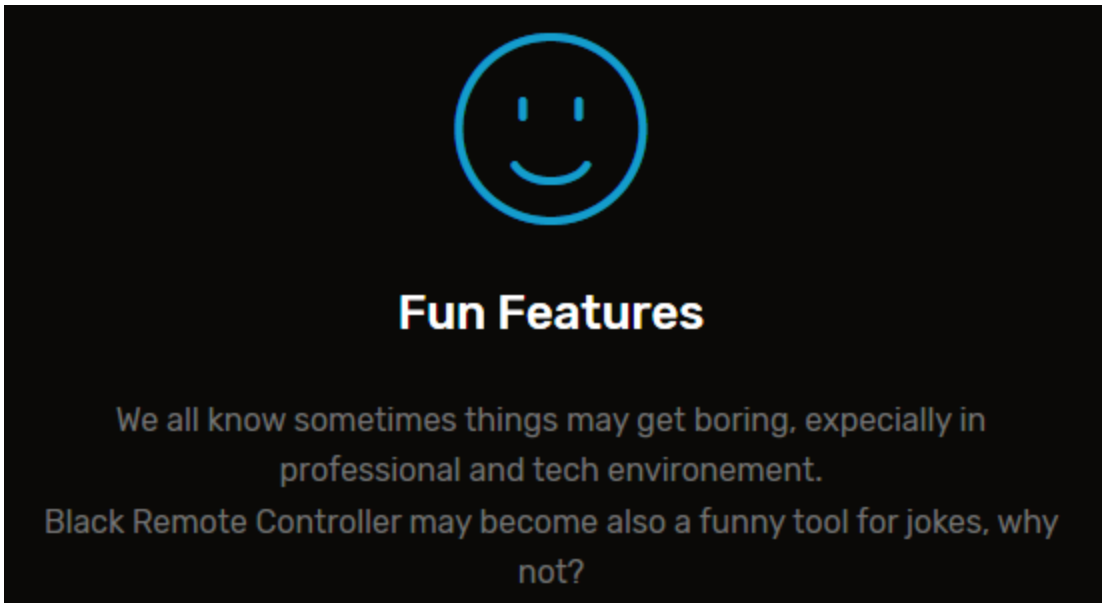


Figure 5. "Fun Features"

Speccy licenses (Figure 6) his RAT at a comparatively high price compared to other commodity RATs. With $49 for a 31-day license, $117 for 93 days, and $438 for one year.

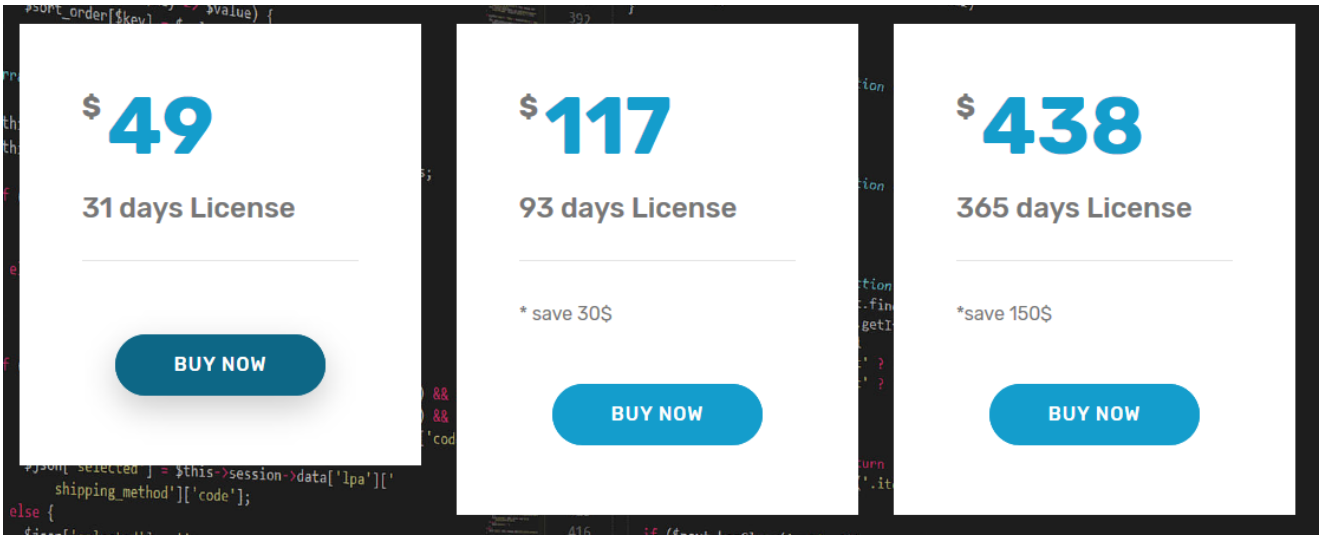


Figure 6. Purchase

The purchase itself is through various cryptocurrencies, using third-party payment service vsell[.]io (Figure 7).

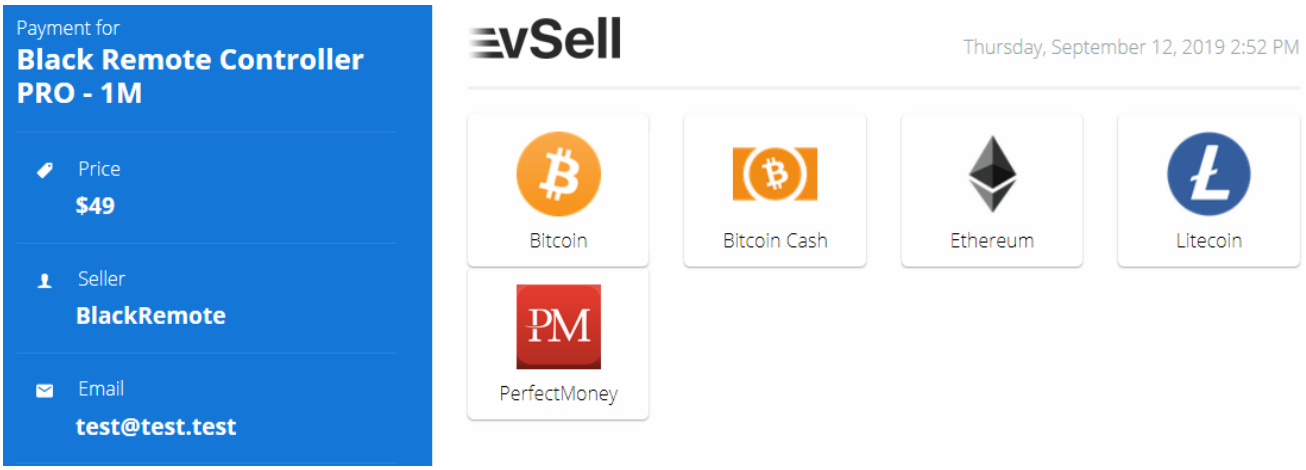


Figure 7. vSell

Features

The site lists the features of this RAT in detail:

"Remote Desktop
Watch the Remote Desktop Live at incredible low latency, take shots or activate video recording to .avi files. Take control over the mouse device and more. Supports multiple screens.

Remote File Manager
Freely navigate in as fast as in real time through all drives, files and folders of your remote machine.
Be able to achieve any kind of file manipulations.

Remote Webcam
Private property surveillance, monitoring, parental control, this feature allows for multiple needs. Take shots or activate video recording to .avi files.

File Transfers
Upload and or Download any data from and to your remote machine. Multiple transfers at once supported and no size limit at incredible speed.

Keystroke Capture
Keystroke capture Live or in Offline mode and retrieve logs later. All keyborads [sic] are supported. A keyword search feature is included.

Services Manager
Be able to list all remote machine stopped and running Services, launch or stop them in a click.

Processes Manager
Monotor [sic] all running Processes in your remote machine, kill. suspend, resume them or set an alarm on specific ones if detected.

Remote Audio
Listen to your remote machine Microphone device, great for surveillance or just listen what the remote user have to say to you.

Registry Editor
Navigate through the full remote machine Windows Registry, retrieve or modify any key or value in it, create new ones.

Chat System
Be able to initialize a Chat session with the remote machine user it for assistance or any given need.

Shutdown, Reboot, Logoff System
Be able to remotely logoff, restart or shutdown your remote machines as needed.

System Messages
Create and fully customize system messages, alerts, infos to pop up on your remote machine.

Downloader
Download and execute any file from a given URL with complete customization of the saving path, execution and more.

Passwords Recovery
Get all saved password in the remote machine, browsers, mail clients and few applications are supported.

TCP Connections Monitor
Monotor all active TCP connections in and out your remote machine. Be able to block them by port, process or instant kill.

Visit Website
Be able to launch any website page for support or any other specific need.

Clipboard Manager
Acces, read or write or edit the remote machine Clipboard content.

Scripting Tool
Create and execute remotely your scripts. VBS, HTML, BATCH, POWERSHELL supported.

Startup Manager
Manage all remote machine System Startup entries. Add, remove, modify them through multiple startup methods.

Remote Shell
Being able to access your remote machine Shell is vital to achieve almost any and advanced task.

Windows Manager
Be able to manage any open windows, visible or hidden ones on your remote machine. Close, maximize, minimize, hide, show, block, any interaction is supported.

Installed Software
Sometimes being able to tell wich software is installed on a system is usefull [sic] to get an idea of how the remote environement [sic] is set.

Hosts File
This file has a critical role for Windows systems, being able to redirect, block, translate, associate ip/hosts addresses. Hosts file customization is sometimes critical to block some websites access for example.

Client Manager
You have plenty of options to modify, update, restart, kill and more of your installed Client file.
Client editor will allow for customizations of your file."

Manager / Builder

The purchaser is given a Sendspace download link for the Blackremote manager / builder software, together with the password for the 6 Mb RAR.

Unpacking the manager / builder installs a 9Mb main executable BLACK-RC.EXE, a pair of resource libraries, and a resource directory with a pair of .wav files.

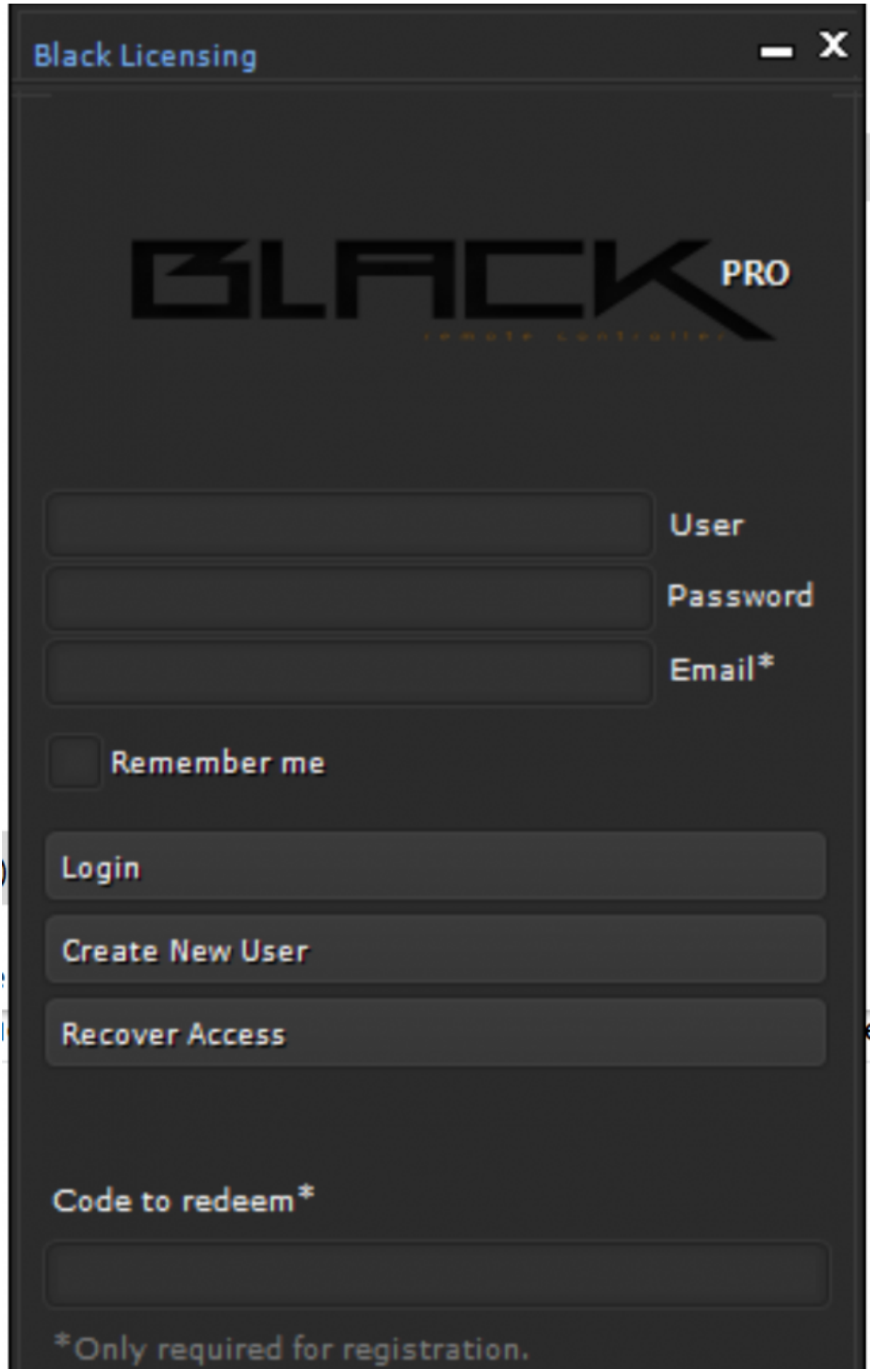

Black Licensing
BLACK PRO
remote controller
User
Password
Email*
Remember me
Login
Create New User
Recover Access
Code to redeem*
*Only required for registration.

Figure 8. Manager / builder registration / login

Upon loading the manager / builder, the user is given a registration / login screen (Figure 8). Blackremote utilizes the third-party “CodeVEST” licensing system, also peddled on underground forums. The licensing system validates by connecting to codevest[.]sh. “CodeVEST” seems to take the place of “Netseal” as a registration service used by commodity malware. The author of “Netseal”, Taylor Huddleston, was charged in 2017 for that operation together with the sale of his own commodity malware, “Nanocore RAT.” The same person who offers the “Codevest” licensing service, also profits from a crypting service “Cyber Seal”. This highlights the role in the commodity malware ecosystem of not only the malware sellers, but also service providers such as the licensing services they use, and the crypting services they purchase to avoid detection of the malware that they build.

Figure 9. CodeVEST

The Blackremote manager / builder (Figure 10) allows the user to build new client malware to their configuration, and to control connections from those infected clients.

Figure 10. Blackremote Manager / Builder

The manager / builder allows the user to define actions-upon-connect for client connections (Figure 11), a connection log (Figure 12), and the ability to list (Figure 13) and interact with connected clients.

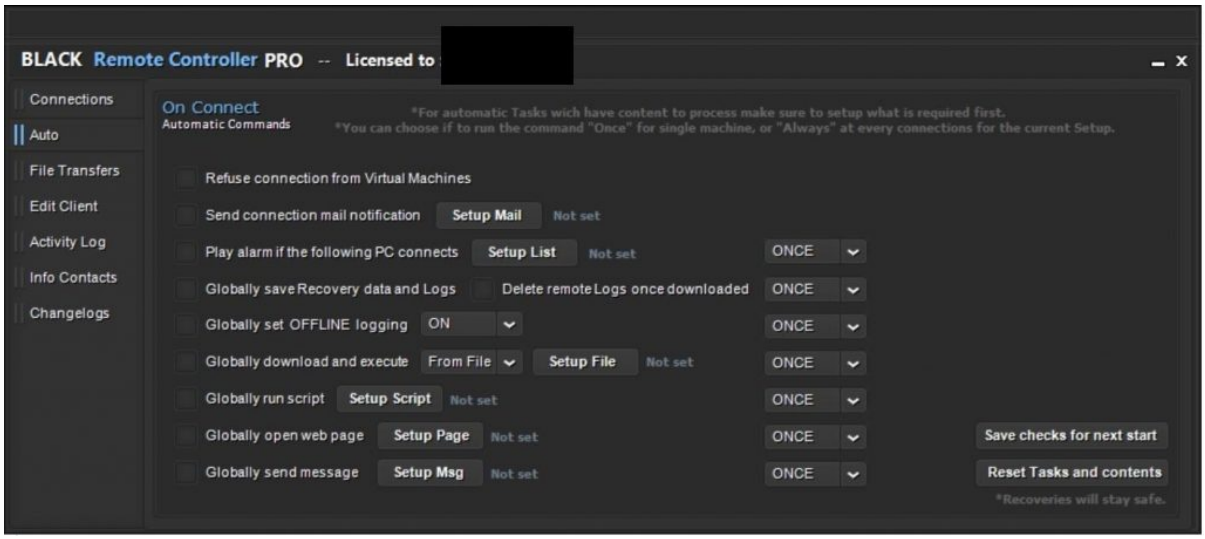


Figure 11. On-connect options

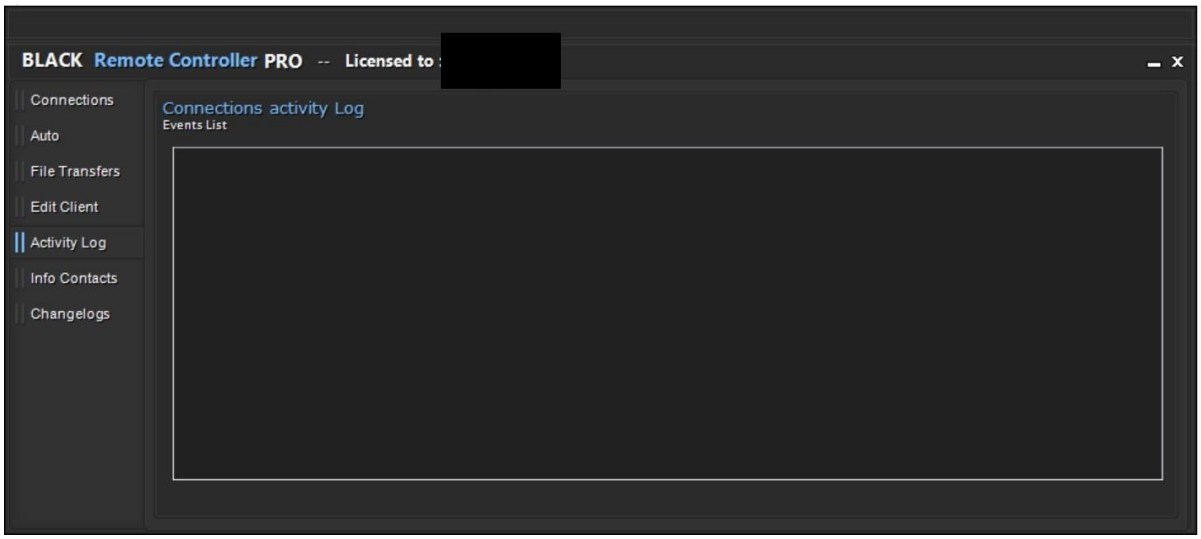


Figure 12. Connection log

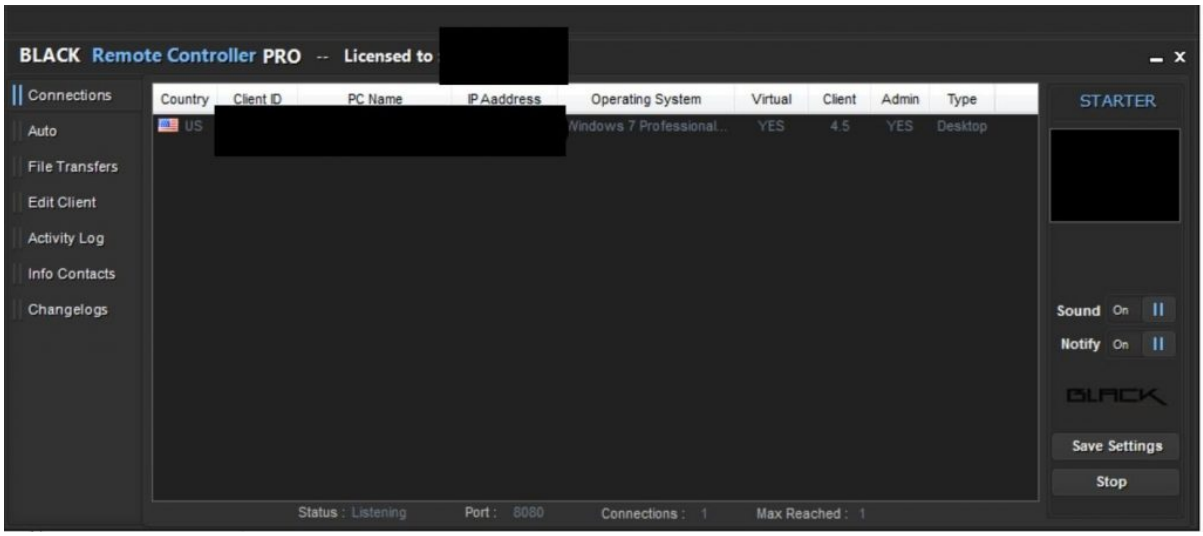


Figure 13. Active connections

The client-control features advertised by Speccy are exposed in the context menu for connected clients (Figure 14).

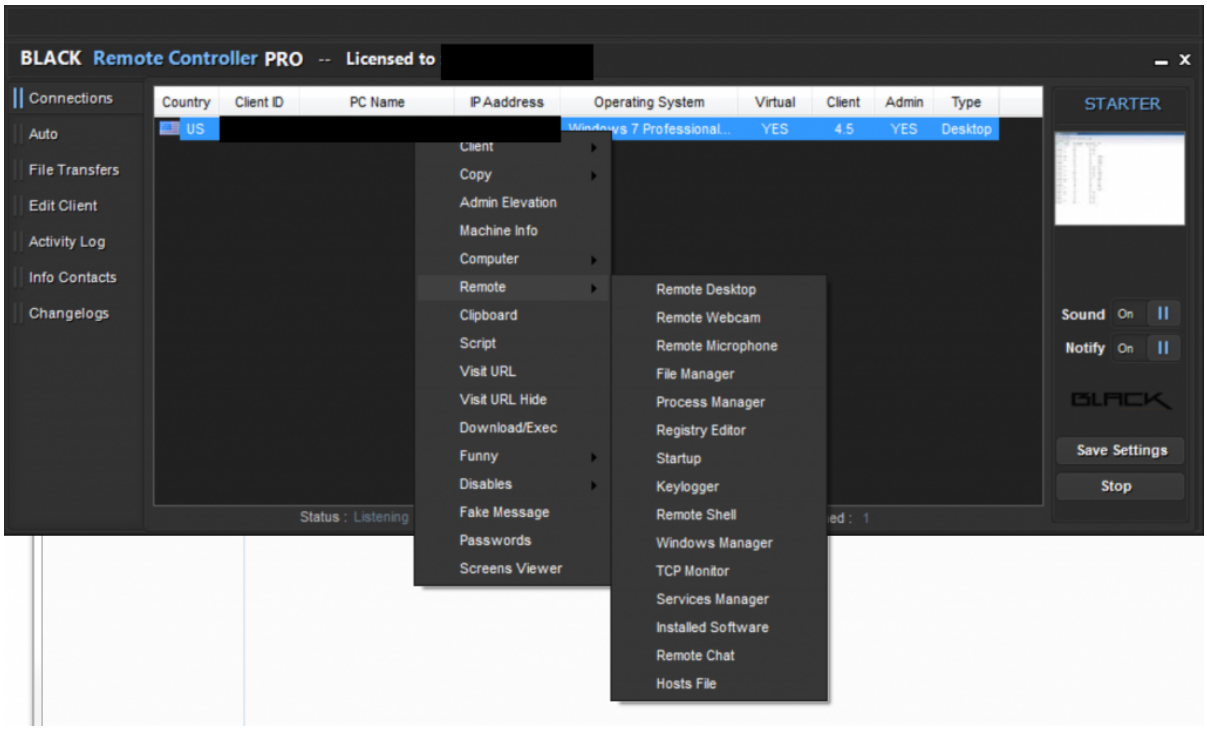


Figure 14. Client control

Speccy is actively developing this software. The changelog shows incremental improvements on a regular basis, such as the newly-added client privilege escalation (Figure 15).

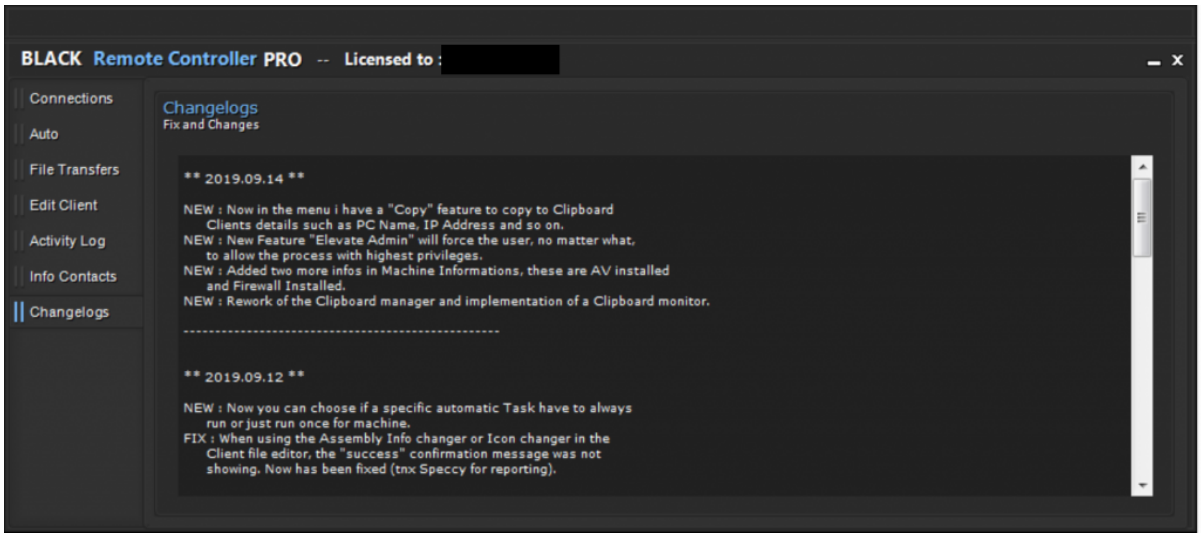


Figure 15. Change log

Client

We note that different samples from similar time periods have been observed with identical file sizes. We suspect that regardless of dynamic content, such as C2 information or differing RAT options, that the obfuscation process in the building of the client may make all clients of a specific Blackremote version level identical in file size.

Both the builder and client are heavily protected, using more than one obfuscator (Agile.NET, Babel .NET, Crypto Obfuscator, Dotfuscator, Goliath.NET, SmartAssembly, Spices.Net, Xenocode).

In the Wild

Although Blackremote is very new, as of the time of this report we are already seeing it used in attacks. A month after Speccy started selling Blackremote RAT, we have almost 50 samples observed in more than 2,200 attack sessions against Palo Alto Networks customers.

A Customer

Interestingly, just one campaign seems to be responsible for the vast majority of those attacks. The file doc00190910.exe (SHA256: 2b3cda455f68a9bbbeb1c2881b30f1ee962f1c136af97bdf47d8c9618b980572), was spread by email, peaking September 9-11, 2019. It targeted Palo Alto Networks customers in varied verticals (Figure 16), worldwide. It uses renaj.duckdns[.]org (103.200.6[.]79) as a Command-and-Control (C2) server. We observed this used in over 1800 attack sessions.

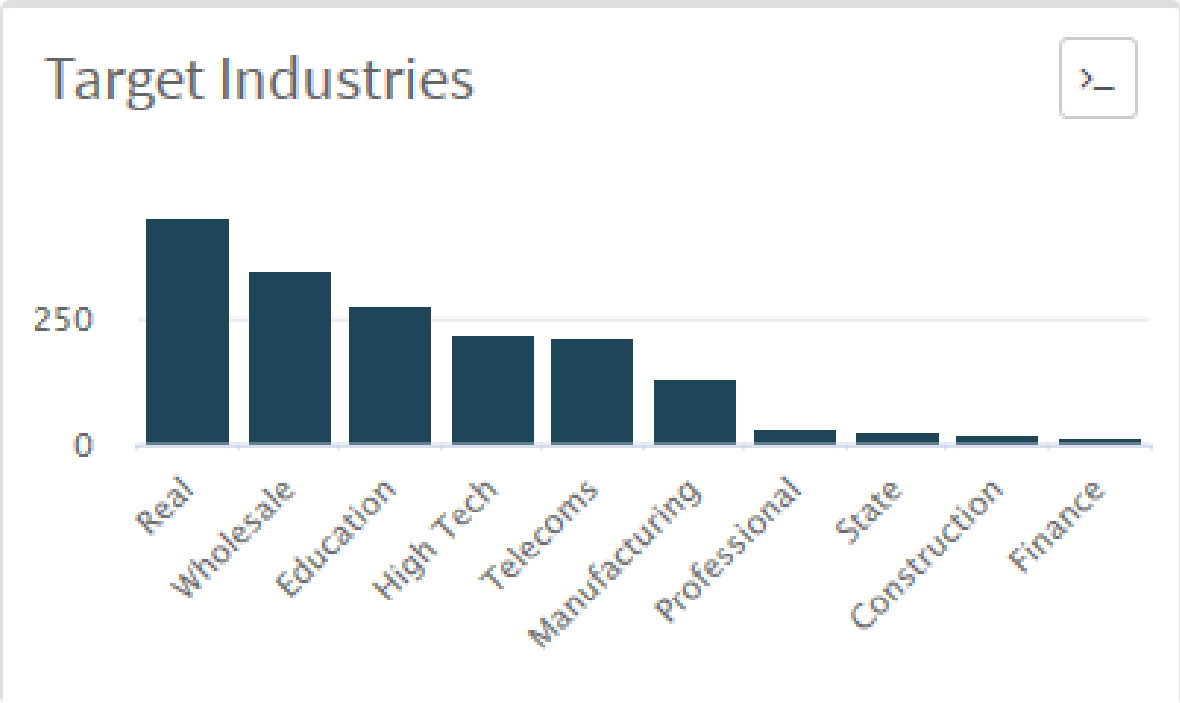


Figure 16. Campaign victim verticals

The same C2 has been observed being used by the actor in over 50 Netwire, Nanocore, Quasar, and Remcos commodity RAT samples back to early 2018.

This is a clear illustration of how the authors of commodity RATs such as Blackremote profit, while enabling malicious cyber attacks.

Conclusion

Commodity RATs are often sold on the internet for years, their authors profiting while enabling malicious actors to spread thousands of samples of malware, built with their RAT builders.

The opportunity to document a RAT within days of its emergence, and to identify the individual behind it – in this case, an 18-year-old from Sweden, will hopefully enable authorities to take timely action against this actor, and his customers. Unit 42 has fully identified this actor; we will not share his identity here, but we have ensured that the correct authorities have been advised. The longer this is sold, not only the more samples of this RAT will be built and spread, but also the opportunity for other actors to crack this RAT and distribute it indiscriminately. It is important to identify and interdict the sale of such malware as early as possible to prevent its proliferation, which enables a large population of unsophisticated threat actors.

Organizations with decent spam filtering, proper system administration, and up-to-date Windows hosts have a much lower risk of infection. Palo Alto Networks customers are further protected from this threat. Our threat prevention platform detects Blackremote malware, with Wildfire and Traps. AutoFocus users can track this activity using the Blackremote tag.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Hashes

514b3d98c1a8cbd5ea08ff31e22700adb9ca0d93d9bc4d6a5232324f0f3e806d
39721fb2d55777eeb6bdfdc9068782894993d172bb92cbad6a525c130312ef11
c3075bced2e864ee7e693c19ecf1ed82cde0aae3d440e9ff2f37d3d6e20fdf0f
3eda427ad5816e6dcf077562a367f71e8bdf5aa931e594416ae445357c12b409
3265bb60b532005bc3535bdf7336bff1845aa5ed3306fd5dbb2ec884cb3d6323
744438c125ceb7a3a7e44cca9fd6b397e982d048f680f164abd46743fd64cd12
33a34ae9a757f6be754571e752a3ee9200153db16c34cf2fd5590ad616fbb04e
fb8b9fe377ccdef76645a081905137e3580eed1defdabbbf48a3d20f0dc760b4
0278145549af5cad9318d51e4c150afe2180b55f72194562885d5c8f9526f465
ea5384db27a27b826c100bbc2535561ea61bf4f44eb4eb93243740188799d675
123539b0eaff1a23606d3716cdc0c73618af6f0cd821ae33863d0f47b2267dbf
f7b165903f6f9b979e84399ce4e1b85ed2927740771d85a7b8c85203641a08a1
93bfbd4b12a17732c8b7e66c554f98187184c6d845bd02e0dbb2104ce8da0453
469d8b2cced859f57b535363307c1e29c0bf0342d14ce0da109a40493a441b62
ada653c948875a9c1ca588251b317d8e971fdf980252d92e36d59f14f5eb9ab9
c207cf50305f126451e2dc5493d83614fdf801541d011e5002ee5daea2b4433b
57a15cc236e4d2ba6e08b062a75671b8a674e0d8498d87e48652c778ea263d49
3875545099276f2b34c3752b177b6d90a2eeb47148ddfb559a4d076d0f40716a
e1bf5d2ef3a4f922f9a15ab76de509213f086f5557c9e648126a06d397117d80
ed7693d9b1b069d39451002bc1df06bf4e123926fa34abb6afeb9a18d6d90dcd
901e06cd91adb7255d75781ef98fac71d17f7bed074a52147bdbd42ea551b34f
9c93b768b5261194ad207c0e92e9767e70ba38203f24f2909e1b39a9a1d6570c
129491bfdd9a80d5c6ee1ce20e54c9fb6deb2c1e1713e4545b24aa635f57a8b9
931839ee649da42b0ee3ac5f5dfa944b506336c7f4e5beb3fc07a6b35a7e6383
0908f8fbe1e3a77d941ae83fe3677d103d86d6e59a6ae4530eadba8af7fc1b3a
69aaaf148a132385512f66d7668b045d6467f8639a3ef7460e20ce0627bc84fc
f6ae66a8a6357d7622463db9953ae164d496e7f5ee0dfe2c8e3550a231f25078
c5a78bf01ab2e44c7dba3a363f2eda51cf648e904f2beb47d6cf3112368ff20c
f83e25cf2b2c2f2d0a14e3f538c11f70135ee8ec158446a51bb0f2d999765267
cb423b73ae3e51195abbcf8bc1f2655d61436825815089b92e843b570ac7c86d

ee20db296c7c4cf3ca6db0c739f1579f554a447b6c1e2b343b22d341f288662f
a4bc7d42dd64df3502b7f8c2335c64eba7a484479fc8c2dc8a4aa448f10354b3
756efcbd2767c5499b6f09a089033c82050459fc2999d3ce79caa25746693e26
117cf46ae69134dbe0c8a1d5f4cac92b46c15ea4945929df3880c0ac63e158f3
e5366365852a953a1747ab8a5d721c2536c5671c07bfecf648fb2cf6a13f2dc0
0c63983cb38d187c187f373852d7b87ff4e41ea0d77d75907aa3388ad957f38f
e54531896dbd100fec41cfc89b06f2afa1efd4077d1f197b1b88f74371135436
c38006115bd7c22151c4e31d8d4ed6ec114c2aaf1c7c0da12ef7b44f96fc58d6
0f66acc9883b284580980020d4a48557b2fe38312ca80db97c77cc2fa78c51fb
77fe670ed011e547db72207ba5849b9f618185b52e0ae766c23ef675b116b252
2b3cda455f68a9bbbeb1c2881b30f1ee962f1c136af97bdf47d8c9618b980572
105cab9c9604238c05be167c6d8d47cd2bc0427b07ede08c5571b581ebd80001
cc795b94cac222afc69749359d8b17d9fb7a7fb6e824d43008c1674c0d146929
1737cf3aec9f56bb79a0c4e3010f53536c36a1fbeeedea81b6d7b66074ecffbe