RAT Trapped? LuminosityLink Falls Foul of Vermin Eradication Efforts

researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/

Simon Conant February 7, 2018

By Simon Conant

February 6, 2018 at 8:15 PM

Category: Unit 42

Tags: Law Enforcement, LuminosityLink

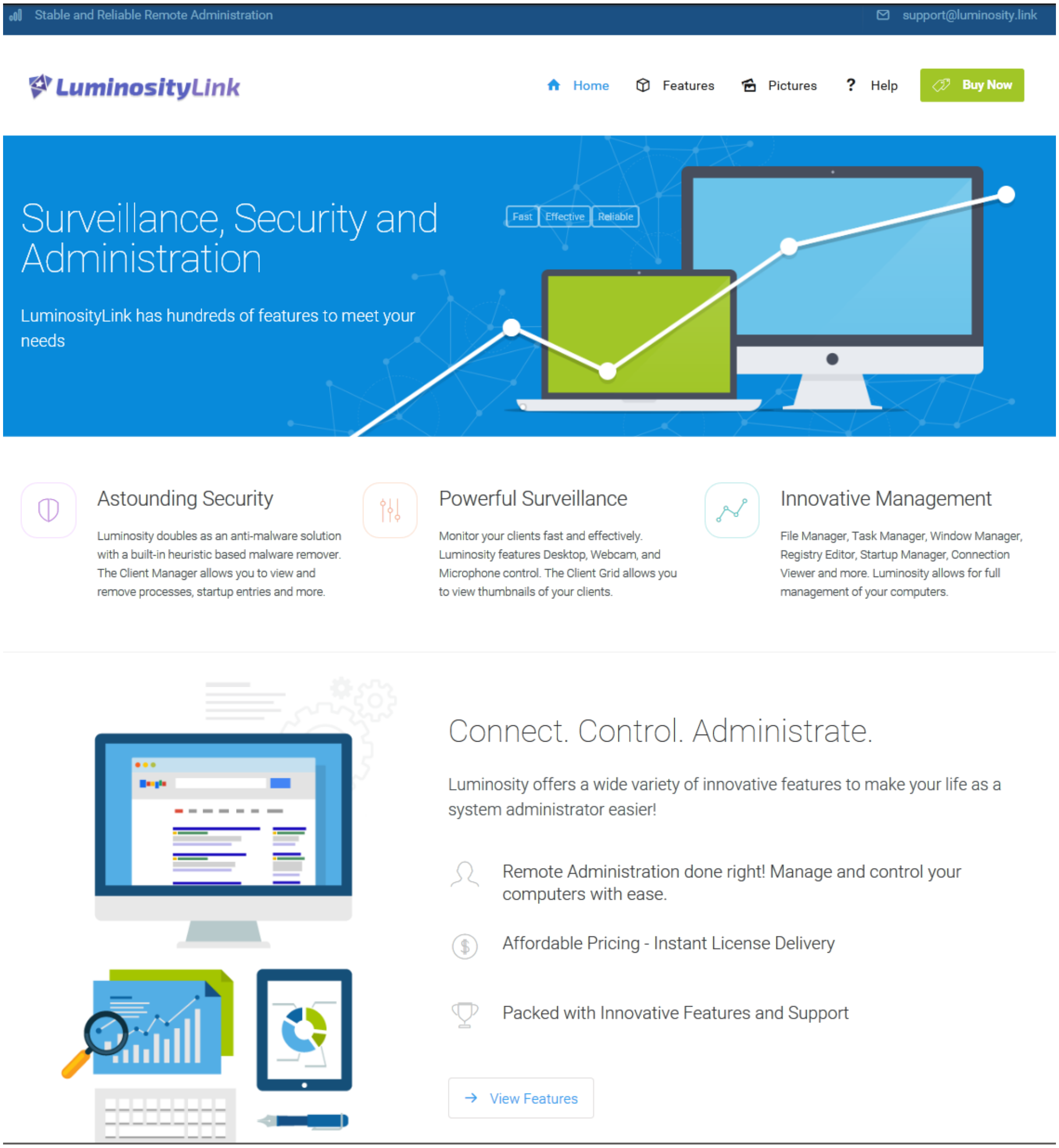
Summary

In July 2016 Unit 42 analyzed the LuminosityLink Remote Access Tool (RAT) which first appeared in April 2015. LuminosityLink was once a popular, cheap, full-featured commodity RAT. Now, however, LuminosityLink appears to have died – or been killed off – over half a year ago.

We recently noticed that the sites luminosity[.]link and luminosityvpn[.]com had been taken down and were looking into the possibility that it was indeed "dead", when we saw on February 5, 2018 Europol published a press release that stated "*A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link.*".

In this blog we look at how LuminosityLink indeed appears to have died, go into some details on LuminosityLink's prevalence, and discuss LuminosityLink's capabilities and how they belie claims sometimes made that it was a legitimate tool.

Up until July 2017, the LuminosityLink RAT software was sold at the website luminosity[.]link (Figure 1).



Surveillance, Security and Administration

LuminosityLink has hundreds of features to meet your needs

Astounding Security

Luminosity doubles as an anti-malware solution with a built-in heuristic based malware remover. The Client Manager allows you to view and remove processes, startup entries and more.

Powerful Surveillance

Monitor your clients fast and effectively. Luminosity features Desktop, Webcam, and Microphone control. The Client Grid allows you to view thumbnails of your clients.

Innovative Management

File Manager, Task Manager, Window Manager, Registry Editor, Startup Manager, Connection Viewer and more. Luminosity allows for full management of your computers.

Connect. Control. Administrate.

Luminosity offers a wide variety of innovative features to make your life as a system administrator easier!

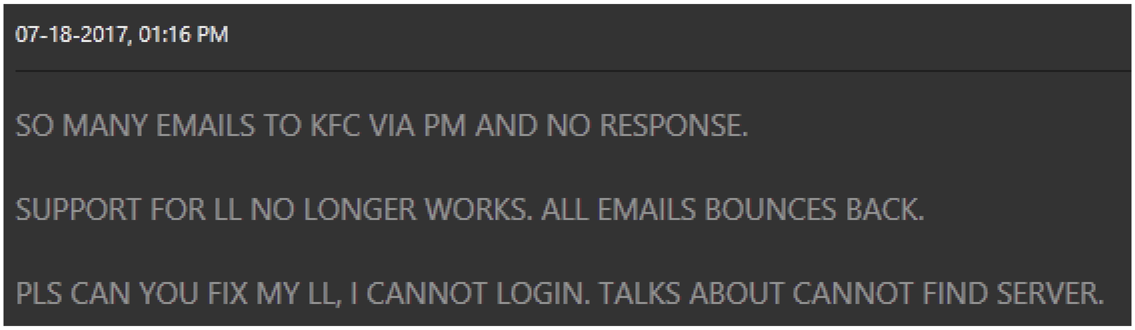
Remote Administration done right! Manage and control your computers with ease.

Affordable Pricing - Instant License Delivery

Packed with Innovative Features and Support

Figure 1 - luminosity[.]link website

Customers complained that their licensing systems were no longer working (Figure 2).



07-18-2017, 01:16 PM

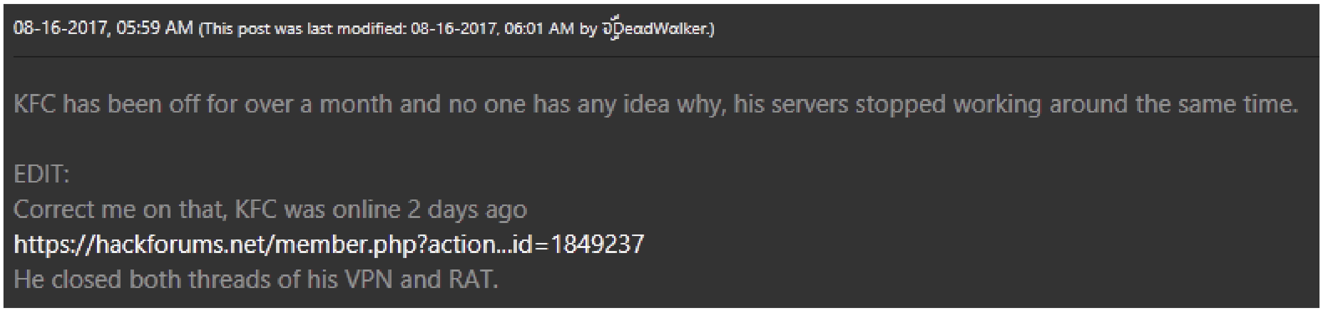
SO MANY EMAILS TO KFC VIA PM AND NO RESPONSE.

SUPPORT FOR LL NO LONGER WORKS. ALL EMAILS BOUNCES BACK.

PLS CAN YOU FIX MY LL, I CANNOT LOGIN. TALKS ABOUT CANNOT FIND SERVER.

Figure 2 - Customers noticing licensing down

The author of LuminosityLink, “KFC Watermelon”, was indeed keeping a low profile – closing his forum thread selling the software (Figure 3).



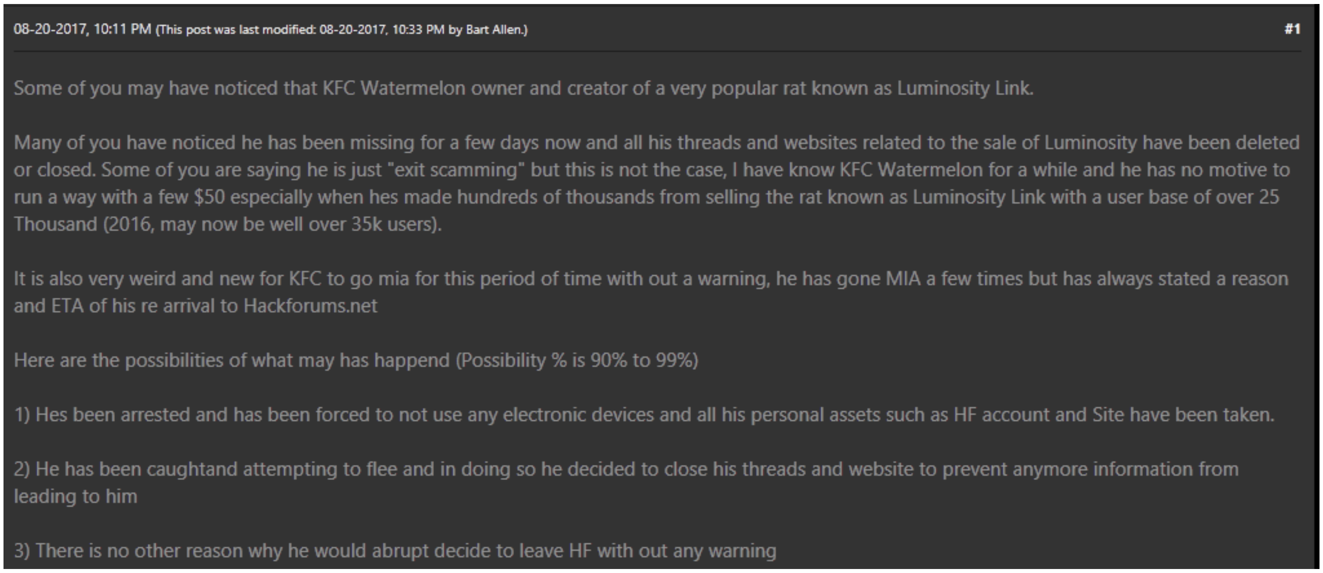
08-16-2017, 05:59 AM (This post was last modified: 08-16-2017, 06:01 AM by จู้DeadWalker.)

KFC has been off for over a month and no one has any idea why, his servers stopped working around the same time.

EDIT:
Correct me on that, KFC was online 2 days ago
https://hackforums.net/member.php?action...id=1849237
He closed both threads of his VPN and RAT.

Figure 3 - KFC Watermelon MIA

As shown in Figures 4 and 5, although unrelated to LuminosityLink, the arrest of the author of the Nanocore RAT earlier in 2017 fueled speculation on forums that the LuminosityLink author had also been arrested and may have handed over his customer list.



08-20-2017, 10:11 PM (This post was last modified: 08-20-2017, 10:33 PM by Bart Allen.) #1

Some of you may have noticed that KFC Watermelon owner and creator of a very popular rat known as Luminosity Link.

Many of you have noticed he has been missing for a few days now and all his threads and websites related to the sale of Luminosity have been deleted or closed. Some of you are saying he is just "exit scamming" but this is not the case, I have know KFC Watermelon for a while and he has no motive to run a way with a few $50 especially when hes made hundreds of thousands from selling the rat known as Luminosity Link with a user base of over 25 Thousand (2016, may now be well over 35k users).

It is also very weird and new for KFC to go mia for this period of time with out a warning, he has gone MIA a few times but has always stated a reason and ETA of his re arrival to Hackforums.net

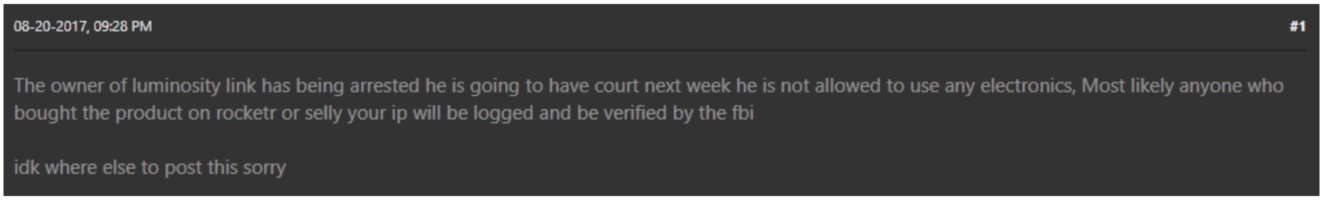
Here are the possibilities of what may has happend (Possibility % is 90% to 99%)

1) Hes been arrested and has been forced to not use any electronic devices and all his personal assets such as HF account and Site have been taken.

2) He has been caughtand attempting to flee and in doing so he decided to close his threads and website to prevent anymore information from leading to him

3) There is no other reason why he would abrupt decide to leave HF with out any warning

Figure 4 - Speculation



08-20-2017, 09:28 PM #1

The owner of luminosity link has being arrested he is going to have court next week he is not allowed to use any electronics, Most likely anyone who bought the product on rocketr or selly your ip will be logged and be verified by the fbi

idk where else to post this sorry

Figure 5 - Arrest

However, even though sales and licensing of LuminosityLink have ceased, despite the rumors, there has been no report of an arrest in the case of the LuminosityLink author to date.

Interestingly, the Europol press release seems to focus upon the *users* of LuminosityLink, and noticeably omits any mention of the author. Our own investigation into the LuminosityLink author suggests that the individual behind LuminosityLink RAT (and previously Plasma RAT) lives in Kentucky. In light of the fact that “KFC” originally stood for “Kentucky Fried Chicken”, the “KFC” in “KFC Watermelon” may have a deeper significance and not be a random handle.

Prevalence of LuminosityLink

Our oldest sample of this malware dates to mid-April 2015, very shortly after the domain luminosity[.]link was registered. In the just-over two years that this RAT was sold, Palo Alto

Networks collected over 43,000 unique LuminosityLink samples through various methods. In total, Palo Alto Networks observed over 72,000 submissions to Wildfire (Figure 6), of over 6000 unique samples, by almost 2500 Palo Alto Networks customers. The most prolific of these individual samples were observed in over 2000 attacks each.

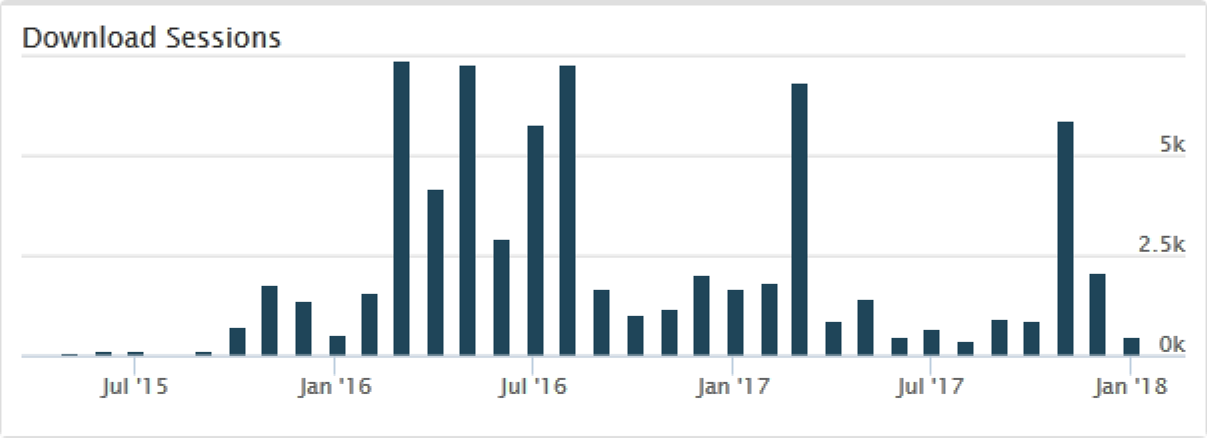


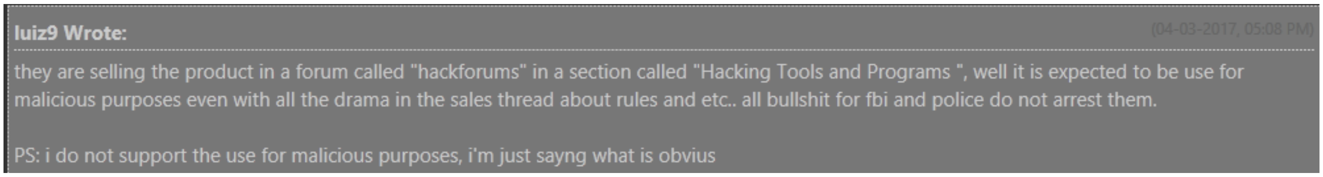
Figure 6 - LuminosityLink Attack Observations

LuminosityLink Command and Control (C2) servers contact the author's licensing server to verify their legitimacy. We note a sharp drop after July 2017, with the licensing server down, though samples continue to be observed. Although we note a couple of noticeable spikes, the observation of new LuminosityLink samples is on a steady decline. Based on other examples, we believe the continued presence LuminosityLink in the wild, even though it's no longer under development, may be due to cracked versions of it being in use.

Malware, or legitimate tool?

Customers of these services, users on underground forums, have expressed concern that arrests of RAT authors might lead law enforcement to their own doors (we see similar sentiments echoed by the customers of DDoS "booter" / "stresser" services).

RAT authors and customers alike claim that RATs represent legitimate "administration tools" – despite the fact that the support thread itself is in under "Hacks, Exploits, and Various Discussions » Hacking Tools and Programs", on a hacking forum (Figure 7).



luiz9 Wrote: (04-03-2017, 05:08 PM)

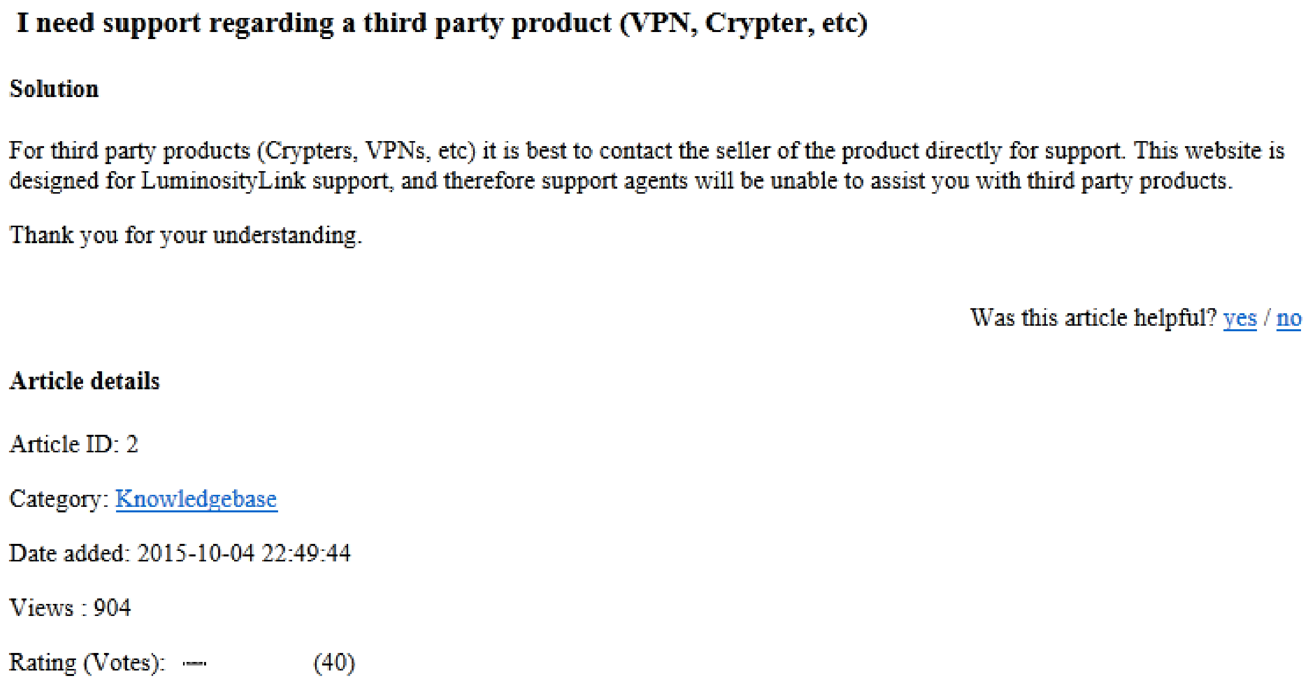
they are selling the product in a forum called "hackforums" in a section called "Hacking Tools and Programs ", well it is expected to be use for malicious purposes even with all the drama in the sales thread about rules and etc.. all bullshit for fbi and police do not arrest them.

PS: i do not support the use for malicious purposes, i'm just sayng what is obvius

Figure 7 - What is obvious

Further undermining these claims, the help forum on the luminosity[.]link site included an article (Figure 8) about "*support regarding a third-party product (VPN, Crypter, etc)*" – suggesting that the use of such detection avoidance techniques was in the front of the mind of the author.

"KFC Watermelon" even states as much on forums "*I do cater to crypter coders now and are in contact with numerous developers to ensure Luminosity works great while crypted. 1.3.1 is further proof of this.*".



I need support regarding a third party product (VPN, Crypter, etc)

Solution

For third party products (Crypters, VPNs, etc) it is best to contact the seller of the product directly for support. This website is designed for LuminosityLink support, and therefore support agents will be unable to assist you with third party products.

Thank you for your understanding.

Was this article helpful? yes / no

Article details

Article ID: 2

Category: Knowledgebase

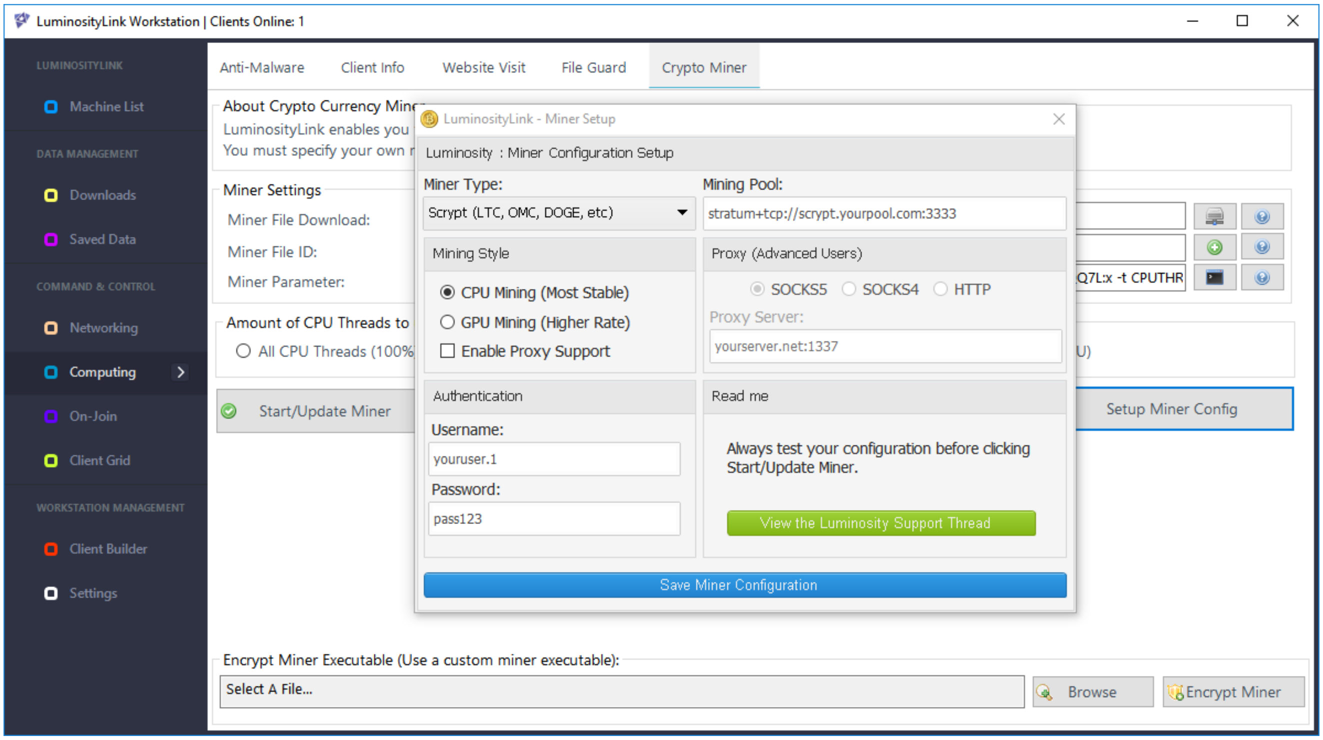
Date added: 2015-10-04 22:49:44

Views : 904

Rating (Votes): (40)

Figure 8 - luminosity[.]link support article

Even more to the point, LuminosityLink boasted feature sets such as "*Surveillance: Remote Desktop, Remote Webcam, Remote Microphone*", "*Smart Keylogger: Records all Keystrokes, Specify Websites and Programs to Record Separately, Keylogger Viewer, Organized and easy-to-use, Search Keylogs Easily*". These all heavily suggest a purpose other than legitimate remote administration. And other features would seem to have no legitimate purpose at all: "*Crypto Currency Miner: Supports Scrypt, SHA256 and More, Custom Miner Support (For Alt Coins), Set amount of CPU to use, Supports CPU and GPU Mining, Proxy Support, Update mining config at anytime*" (Figure 9).


LuminosityLink Workstation | Clients Online: 1

About Crypto Currency Mine
LuminosityLink enables you
You must specify your own r

Miner Settings
Miner File Download:
Miner File ID:
Miner Parameter: Q7L:x -t CPUTHR

Amount of CPU Threads to
○ All CPU Threads (100% U)

LuminosityLink - Miner Setup
Luminosity : Miner Configuration Setup

Miner Type: Scrypt (LTC, OMC, DOGE, etc)
Mining Pool: stratum+tcp://scrypt.yourpool.com:3333

Mining Style
● CPU Mining (Most Stable)
○ GPU Mining (Higher Rate)
☐ Enable Proxy Support

Proxy (Advanced Users)
● SOCKS5 ○ SOCKS4 ○ HTTP
Proxy Server: yourserver.net:1337

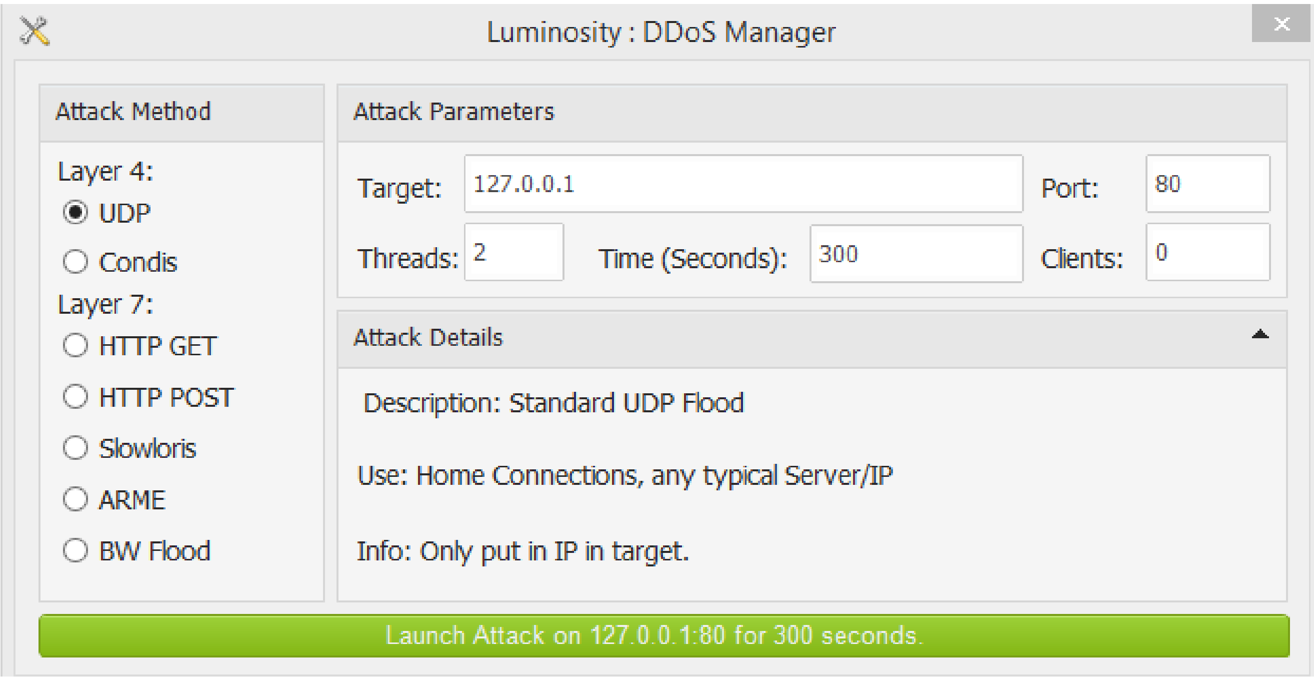
Authentication
Username: youruser.1
Password: pass123

Read me
Always test your configuration before clicking Start/Update Miner.

Encrypt Miner Executable (Use a custom miner executable):
Select A File...

Figure 9 - Coin Miner

It's also hard to imagine a legitimate-use scenario for launching a DDoS attack (Figure 10):



Luminosity : DDoS Manager

Attack Method

Layer 4:
● UDP
○ Condis

Layer 7:
○ HTTP GET
○ HTTP POST
○ Slowloris
○ ARME
○ BW Flood

Attack Parameters

Target: 127.0.0.1
Port: 80
Threads: 2
Time (Seconds): 300
Clients: 0

Attack Details

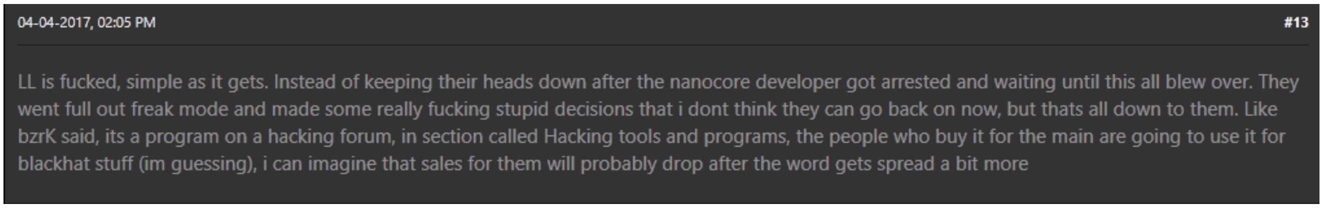
Description: Standard UDP Flood

Use: Home Connections, any typical Server/IP

Info: Only put in IP in target.

Figure 10 - DDoS feature

Per “KFC Watermelon” himself “*I also re-coded the DDoS modules in 1.0.0.1 and made the Layer 7 attacks more effective.”.*
Another forum was quite accurately prophetic about the risks the author of LuminosityLink was taking in April 2017, about three months before the site was parked (Figure 11).



04-04-2017, 02:05 PM #13

LL is fucked, simple as it gets. Instead of keeping their heads down after the nanocore developer got arrested and waiting until this all blew over. They went full out freak mode and made some really fucking stupid decisions that i dont think they can go back on now, but thats all down to them. Like bzrK said, its a program on a hacking forum, in section called Hacking tools and programs, the people who buy it for the main are going to use it for blackhat stuff (im guessing), i can imagine that sales for them will probably drop after the word gets spread a bit more

Figure 11 – Forum Comment on Risks LuminosityLink Author Was Taking

Conclusion
Based on our analysis and the recent Europol announcement, it does seem though that LuminosityLink is indeed dead, and we await news of what has indeed happened to the author of this malware. In support of this, we have seen LuminosityLink prevalence drop significantly and we believe any remaining observable instances are likely due to cracked

versions.
Finally, a review of most recent feature sets and capabilities for LuminosityLink show that even if some of its capabilities could be put to legitimate purposes, taken as a whole, the preponderance of questionable or outright illegitimate features discredit any claims to legitimacy.

Coverage

Palo Alto Networks customers are protected from this threat in the following ways:

1. WildFire accurately identifies LuminosityLink RAT samples as malicious.
2. Traps prevents this threat on endpoints, based upon WildFire prevention.

AutoFocus users can view LuminosityLink RAT samples using the “LuminosityLinkRAT” tag.
IOCs can be found in the appendices of this report.

Appendix I – Top 20 samples

07b4b11940baa619c0c6ec91b1a73715f4a1ece29ad85287b7db97718a60aea5	2260
efdf2238c091f4ff3fa9b2eea8cfa5c9edad70434fc81cba5a81d2b3fe188276	2142
73f7967d53fe124a028311db97b2b1c0a53acffe269c37d20e31f2a4a068ab28	1769
45657413799e9481eff4c83bf183b9343b3f7ed1ecde6724b1a7d2c2c6e4839c	1260
df5a90d5dac6c3a4286230e0b0d4835ec936b11bbacf6b031b25ff6545ed153e	1007
8785ef18b75605bd659a346ec890b4888749c6015b729cd3363fd8289e55faf3	959
f3aacd6a47fd6655408507446ff53b946108f29e2a3dc0bb2f496b8e36927ce7	890
add98a6912601551634239a6867ea10136fd6cf770cd25eecde576a3853738d8	823
c4eee35f0e51a04a7daca1431c4926d02720590ce62200c8362bacc66eb574b1	764
53d817e8a824488a622cf653c9d48164c3d741aa19f2e2d89a713005f81109ef	751
a3dd71e5bd2d9edad31252d3d6049b5ffb1d6bd11fe6215f9d2c8cf093ba8ab7	749
82151d68ae5ec5e00e81998785371ff694b37bfe6093fe3bd8c9932ed21651c7	731
68a599d2658096ff9c529c5aeb9644119c47e1c744b07323a3df8a8e5e94c4da	725
1f79ac7f0201584d6ea7d6b0c96d2285572ed4a191e765a20f5ccae6ebb2f34d	718
50349613c6fbac2b344f5b7753a165620be112a674763153a6de497df43589af	712
79a6a3c5ae196a1874234f5870fc8c6d07059c85cb1fca73d21c8eb51c0d41b1	680

8329f8176e926053fc9a4db2f9eb09aff6fec31c197e919ae26cb9501926c516	674
f8f58cc1095ea29e2c365fa64fdccdebce5113b44e3d7032e96f0ebb3dfd5e9c	669
09681a9054f9f04e270b0ae390c7b697748405d4c29a589ff45a4b485baa18c4	652
0247b0ecbf6069e38e772ef546e63c46262cc77efe5d004a3ec516baf0e74d87	524

Appendix 2 – full sample hash list
A full list of SHA256 hashes for all known LuminosityLink samples, as of 1 February 2018, can be found here.