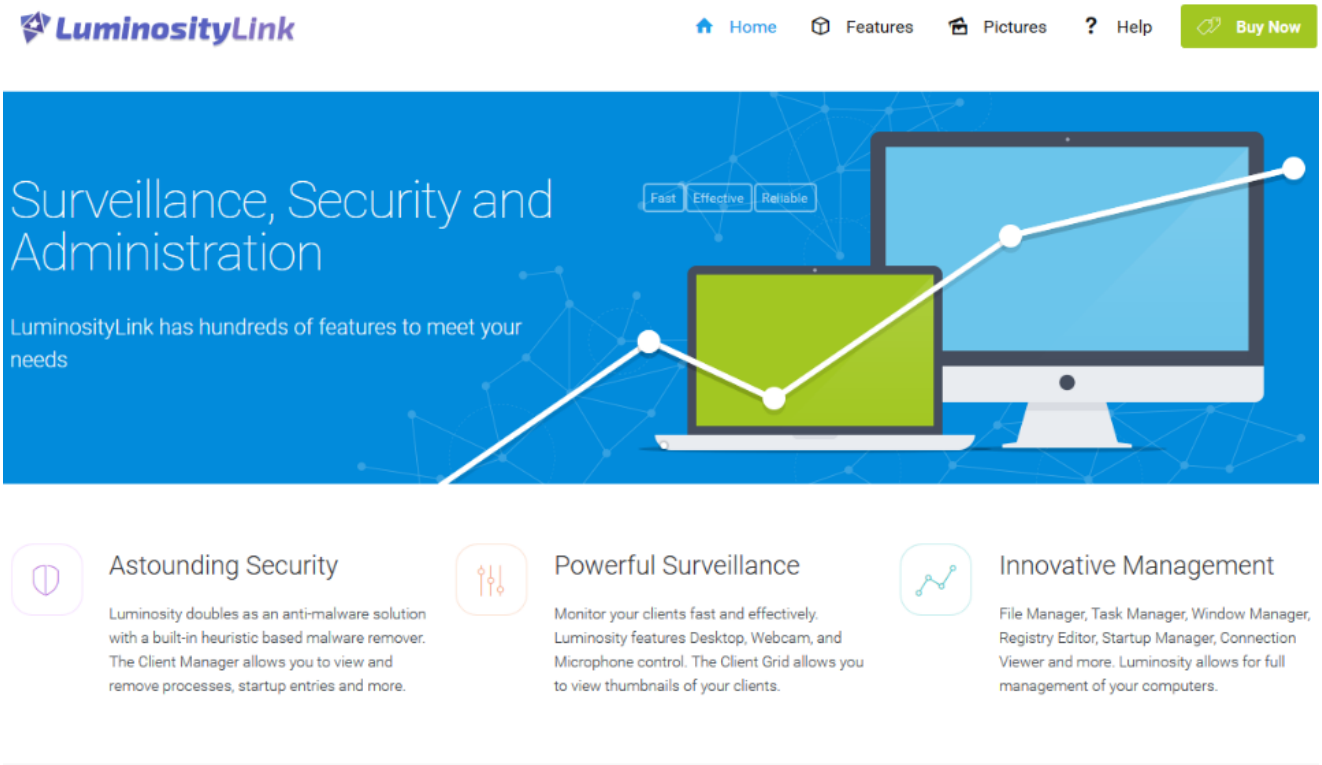
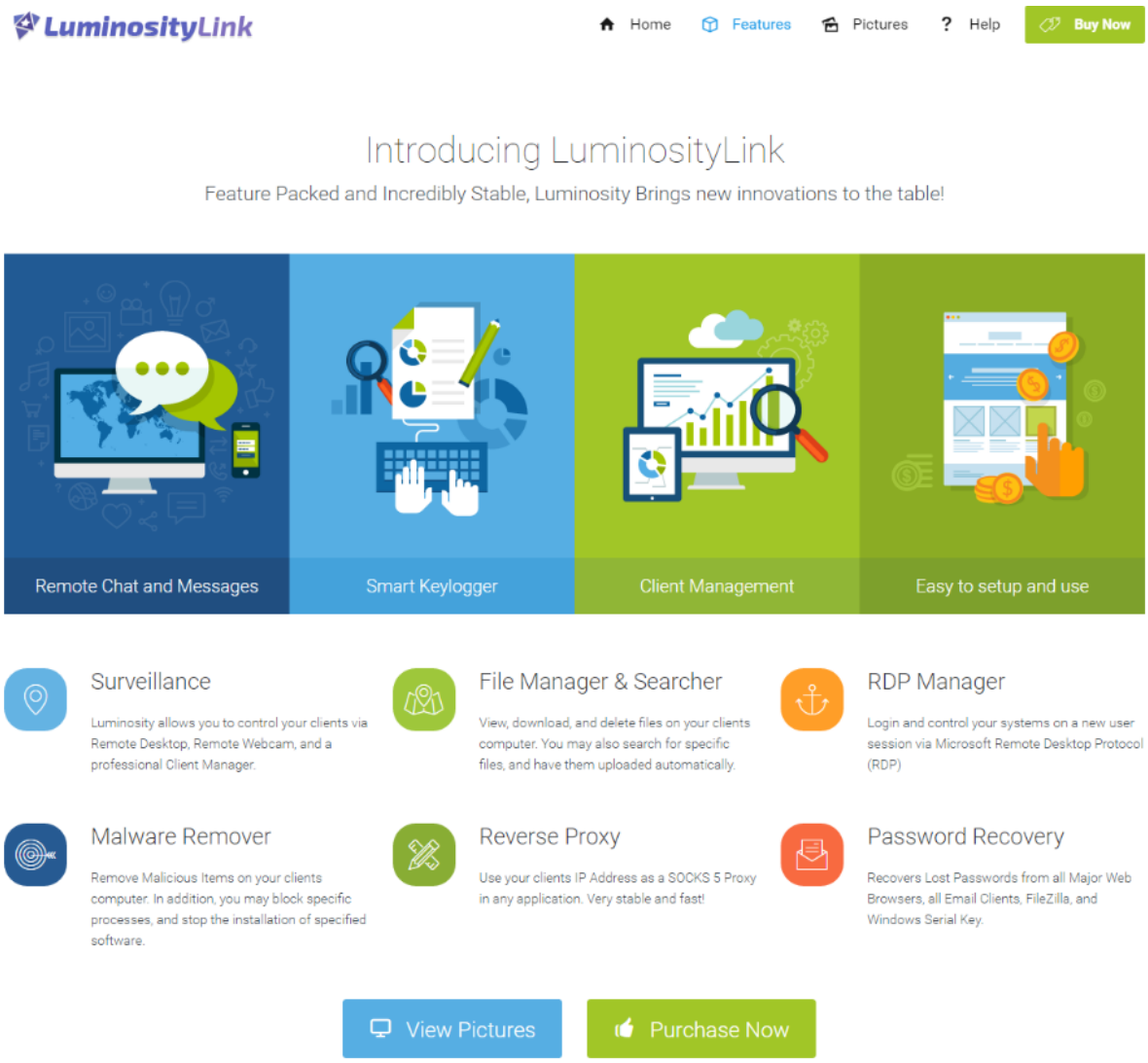
‘LuminosityLink RAT’ Author Pleads Guilty

krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/



A 21-year-old Kentucky man has pleaded guilty to authoring and distributing a popular hacking tool called “**LuminosityLink**,” a malware strain that security experts say was used by thousands of customers to gain unauthorized access to tens of thousands of computers across 78 countries worldwide.

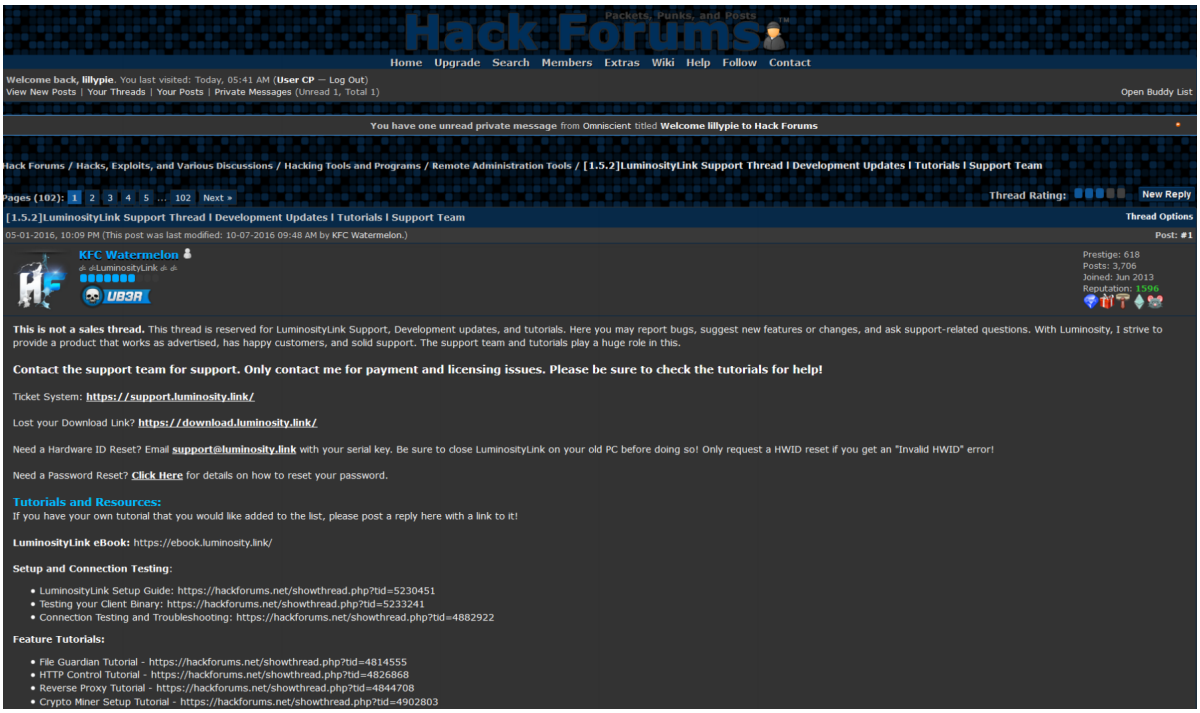


The LuminosityLink Remote Access Tool (RAT) was sold for $40 to thousands of customers, who used the tool to gain unauthorized access to tens of thousands of computers worldwide.

Federal prosecutors say **Colton Ray Grubbs** of Stanford, Ky. conspired with others to market and distribute the LuminosityLink RAT, a $40 **R**emote **A**ccess **T**ool that made it simple for buyers to hack into computers to surreptitiously view documents, photographs and other files on victim PCs. The RAT also let users view what victims were typing on their keyboards, disable security software, and secretly activate the webcam on the target's computer.

Grubbs, who went by the pseudonym "**KFC Watermelon**," began selling the tool in May 2015. By mid-2017 he'd sold LuminosityLink to more than 8,600 customers, according to Europol, the European Union's law enforcement agency.

Speculation that Grubbs had been arrested began surfacing last year after KFC Watermelon stopped responding to customer support queries on Hackforums[dot]net, the Web site where he primarily sold his product.



Grubbs, using the hacker nickname “KFC Watermelon,” advertised and sold his RAT via Hackforums.net.

The sale and marketing of remote access tools, also known as remote administration tools, is not illegal in the United States, and indeed there are plenty of such tools sold by legitimate companies to help computer experts remotely administer computers.

However, these tools tend to be viewed by prosecutors instead as “**R**emote **A**ccess **T**rojans” when their proprietors advertise the programs as hacking devices and provide customer support aimed at helping buyers deploy the RATs stealthily and evade detection by anti-malware programs.

According to the indictment against him, Grubbs “recruited and encouraged co-conspirators to answer questions on Skype, an internet messaging service, from potential and actual purchasers of LuminosityLink seeking to use the software to get unauthorized and undetected access to victim computers and steal information.”

Linking Grubbs to LuminosityLink was likely not a tall hurdle for prosecutors. A public filing at the **Kentucky Secretary of State** office lists Grubbs as the owner of **Luminosity Security Solutions LLC**.

However, there are indications that Luminosity was not Grubbs’ first foray into making and selling malware tools. According to a February 2018 blog post by **Palo Alto Networks**, the Skype account connected to KFC Watermelon’s identity on Hackforums is tied to the email address “codyjohnson1337@live.com; that email account was used in 2013 to register “plasmarat.pw,” a similar RAT sold and marketed on Hackforums.

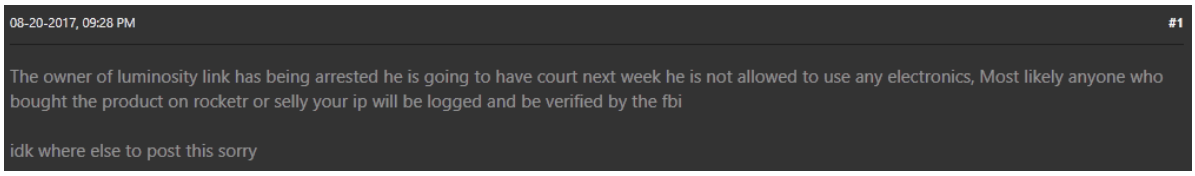
KFC Watermelon's Skype profile (the "HF" in his Skype name is a likely reference to HackForums, where both Luminosity RAT and Plasma RAT were primarily sold and marketed).

The street address listed by the Kentucky Secretary of State's office for Luminosity Security Solutions (127 Circle Dr., Stanford, KY) shows up in the original registration records for dozens of domains, including at least a half-dozen that early on listed the email address **coltongrubbs@gmail.com**. That same email address appears in the early registration records for barracudasec[dot]com, a domain that as far back as 2012 was identified as a popular "command and control" server that many denizens of Hackforums used to remotely administer large numbers of remotely commandeered computers or "bots."

Around the time that KFC Watermelon stopped responding to support requests on Hackforums, federal prosecutors were securing a guilty plea against **Taylor Huddleston**, a then 27-year-old programmer from Arkansas who sold the "**NanoCore RAT**." Like Grubbs, Huddleston initially pleaded not guilty to computer intrusion charges, arguing that he wasn't responsible for how customers used his products. That is, until prosecutors presented Skype logs showing that Huddleston routinely helped buyers work out how to use the tools to secretly compromise remote computers.

Grubbs' guilty plea could well lead to further arrests and prosecutions of customers who purchased and used LuminosityLink. Case in point: The author of the **Blackshades Trojan** — once a wildly popular RAT sold principally on Hackforums — was arrested along along with dozens of his customers in a global law enforcement sweep in 2014.

Indeed, many former customers of LuminosityLink have posted to Hackforums that they are expecting similar treatment:



Hackforums users speculate that Grubbs' arrest could lead to the arrest and prosecution of his customers. Image: Palo Alto Networks.

Grubbs initially pleaded not guilty, and his trial was slated to begin in August. But in a plea agreement released today, Grubbs admitted to conspiring to make and sell LuminosityLink, and to knowingly assisting customers in using his software to break into computers.

The plea agreement notes that on July 10, 2017, when Grubbs found out the FBI was about to raid his apartment, he hid the phone and debit card tied to his Bitcoin account, and also removed the hard drives from his computer and apartment prior to the search. "Three days later, Defendant transferred over 114 bitcoin from his LuminosityLink bitcoin address into six new bitcoin addresses," the agreement states.

The charges to which Grubbs has pleaded guilty carry punishments of up to 25 years in prison and as much as $750,000 in fines, although any sentence the judge hands down in this case may be significantly tempered by U.S. Sentencing Guidelines.

A copy of the plea agreement is available here (PDF).