Finding the RAT's Nest

umbrella.cisco.com/blog/2017/01/18/finding-the-rats-nest/

January 18, 2017

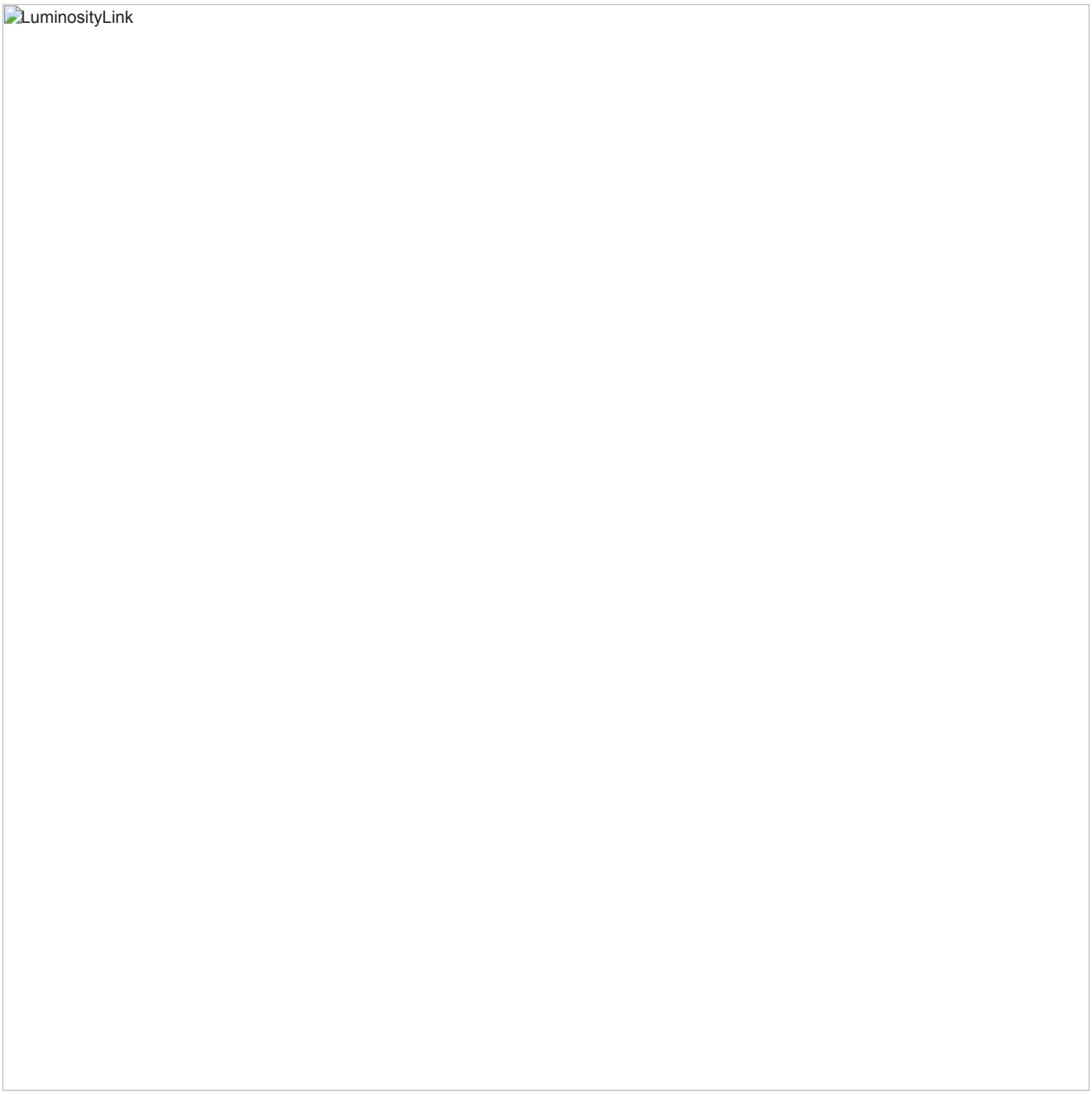
We've spotted a Remote Access Trojan(RAT) and are headed down into the unknown. In this blog post we're going to examine some malicious infrastructure that we've found by pivoting through domains delivering and communicating with RATs.
A RAT is malware that creates a back door to gain access to the target and its connected resources in order to spy/steal information, drop additional malware such as ransomware, or to enlist the target into a botnet for DDoS purposes. A RAT can basically give all of the same access to a system that the attacker would have if they were physically accessing the target. A RAT has many functionalities: remote desktop control, webcam and microphone control, keylogger, remote shell, crypto miner, download and execute functionalities, screen capturing.

Purchase and Preparation

When deciding on which RAT to setup and spread, there is a choice between free or paid varieties. There are RATs that are free to use and RATs that require one to pay for a license. They vary in their ease of setup and stability. Since these RATs have been available for years and are detectable through signatures, a "crypter" is used on the malware before deployment. Crypters are tools that can use encryption and obfuscation on the malware in an effort to make them FUD (Fully UnDetectable) against known pattern based or behavior based signatures used in Anti-Virus or IDS/IPS systems. When a low detection rate is reached they have a better chance of infecting targets. The goal is to appear to be a harmless program. Once crypted, criminals run the file through underground scan services that will tell them their file's achieved detection rate.
The ease of setup and availability of these RATs have helped them remain a threat. There are also rental services, offering to do all of the setup needed to build the infrastructure for RATs and bots, and then rent the use of them for a price.

Advertisement for RAT and Botnet Setup Services

LuminosityLink is widely considered by some cyber criminals to be one of the best RATs. When searching for only one AV signature from Malwarebytes, Backdoor.LuminosityLink, in Virustotal with a First Submission date of the last 30 days; there were 147 *new* submissions. On our resolvers, we see active traffic to the Command and Control (C2) panels and infrastructure behind these RATs.

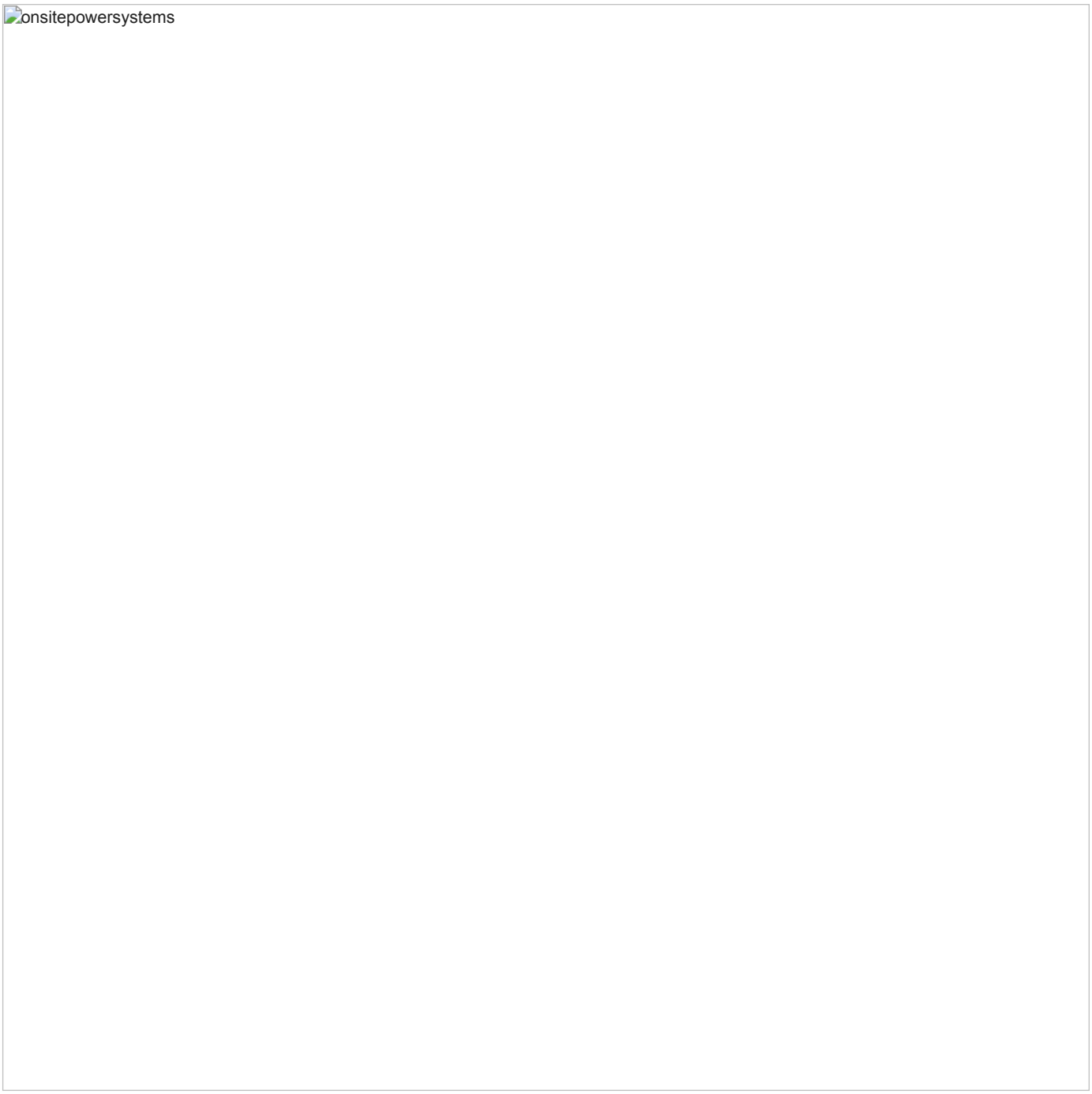


LuminosityLink

Let's investigate some infrastructure around this paid RAT, LuminosityLink.

In The Wild

LuminosityLink is seen here dropped from this site, ***http://onsitepowersystems[.]com/invoice86291320[.]zip***, which appears to be exploited with the C99 Shell. The delivery method is a bit.ly link leading to the zip file at ***onsitepowersystems[.]com***. The C2 communications are at ***191.101.22[.]47***.



LuminosityLink ZIP on compromised website

The bit.ly link as well as the ***onsitepowersystems[.]com*** zip file are still active at the time of this analysis.

As a side note, OpenDNS offers the optional filtering of the URL Shortener category on your network. While URL shorteners are not malicious by design, removing access to them can help protect your users from clicking on links that will redirect them to unexpected places.

Bit.ly redirect to LuminosityLink download

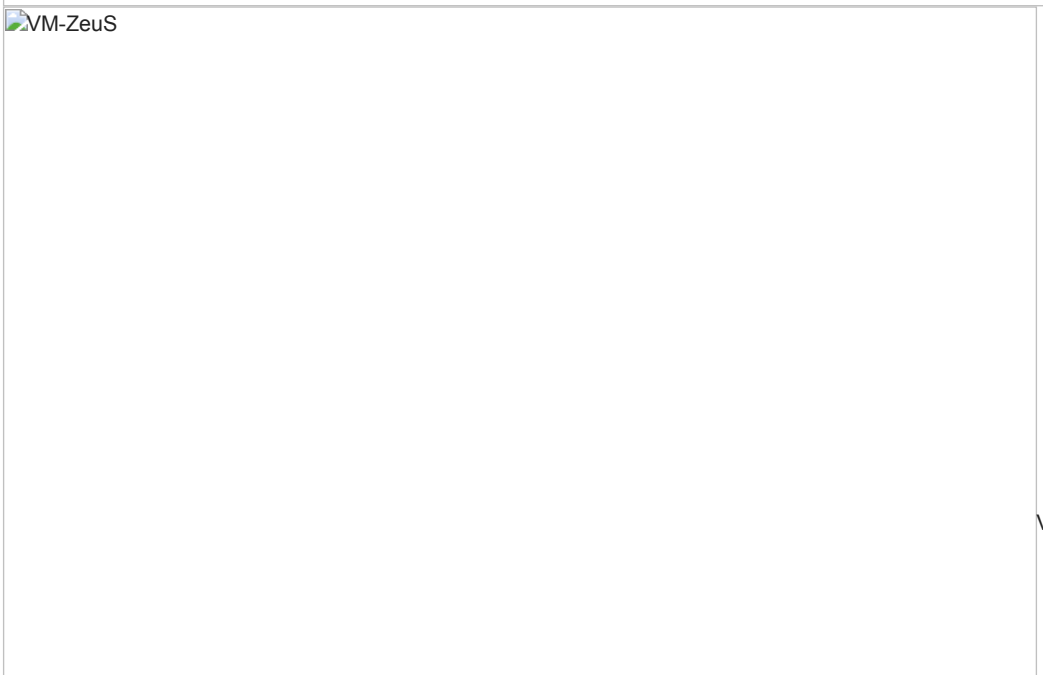
LuminosityLink Executable

*Above sample **083bb90a33710585883ae6bbb7f36437c083a5d889a3e4e3994955a53bfa1be0***

On and On…

Here are a few more C2 panels and associated traffic we've recently seen coming through our resolvers.
thevm2[.]biz and ***blackhills[.]ddns[.]net***
thevm2[.]biz– C2 panel for VM-ZeuS aka KINS (malware that was part of Avalanche) seen with traffic from a LuminosityLink sample and domains associated with Ramnit (a banking trojan).
This RAT is dropping additional malware; utilizing it's download and execute functionality.
0247b0ecbf6069e38e772ef546e63c46262cc77efe5d004a3ec516baf0e74d87
1ae134e146c43891a6e28d917d9cfcf32bb0ff435051261462b57181320b992a
ac3ade715adafa5784c43f407843bf8889e7c97c4e62239c1b22f07aab2920c9

thevm2[.]biz



VM-ZeuS

Traffic seen on OpenDNS resolvers

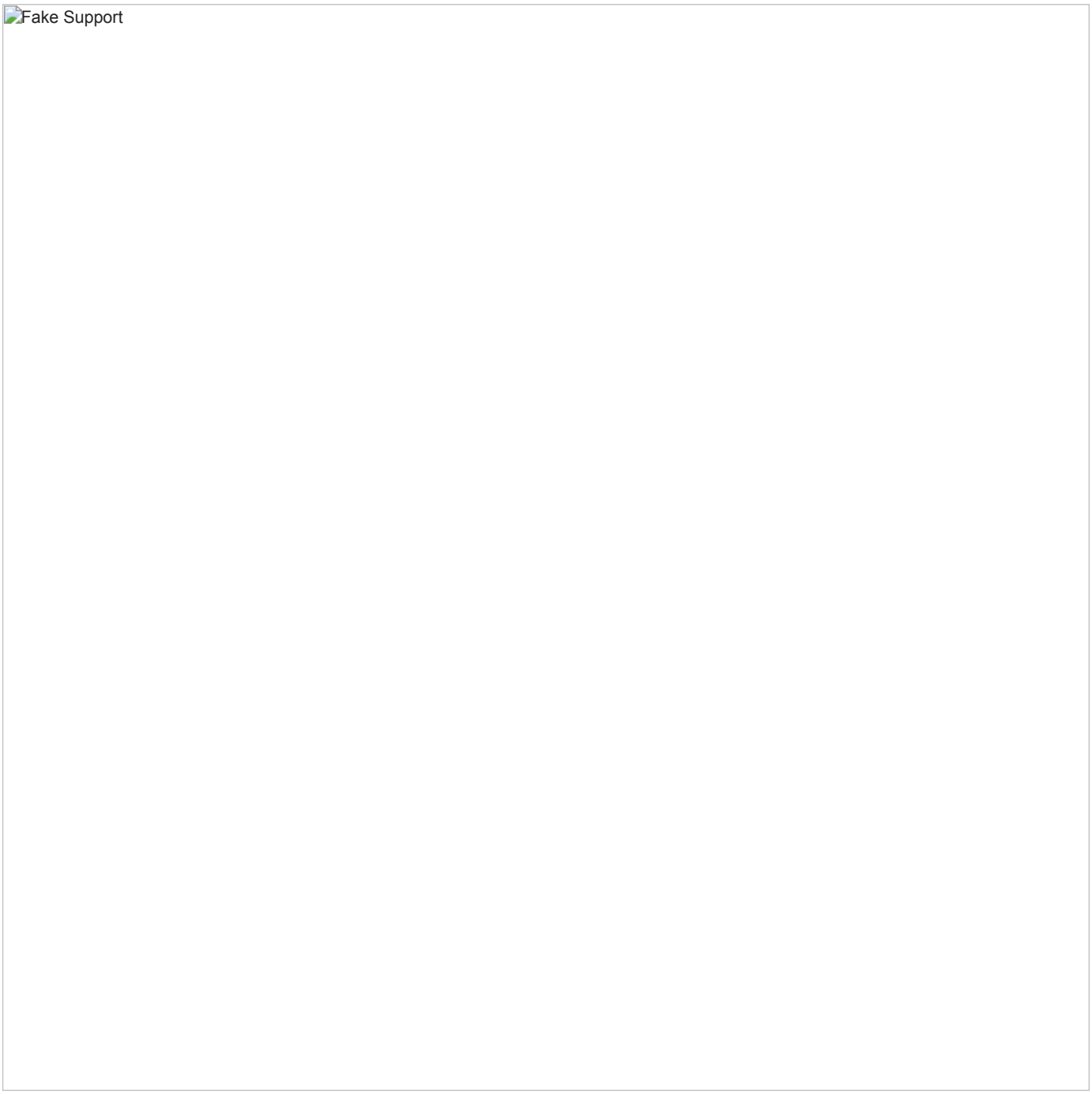
The email address ***nie0461@gmail[.]com*** is the registrant for ***thevm2[.]biz*** and the following domains.

marciaguthke[.]com

email-hosting[.]us

emailhostings[.]in
myvm2[.]biz
thevm2[.]biz
vm2online[.]biz
We're blocking ***hackcom[.]org*** which has the nameservers that are hosting these panels currently, and hosted some in the past. Pivoting through these registrant's domains, we find more malicious infrastructure.
vm2online[.]biz – more panel configs

vm2online[.]biz
marciaguthke[.]com – redirected to a fake Microsoft support page



Fake Support

This domain ***virus-os-77h7ft[.]pw*** is hosted on ***192.111.155[.]6***, which hosts tons of fake AV support domains. By blocking this IP address, we prevent access to all of these domains.

Known domains from 192.111.155[.]6 as seen on our resolvers

From RATs, to banking trojans, to fake support domains. Due to a RATs ability to drop additional malware and the criminals utilizing different delivery methods, we've found a wide range of infrastructure and traffic comingling. By fully understanding the traits of the attack, we can make the most effective counter to protect our customers.