#FAIL #MALWARE

AUGUST 18, 2011

Shady RAT: Shoddy RAT.

Last week, Congresswoman Mary Bono Mack (CA-45), Chairman of the House Subcommittee on Commerce, Manufacturing and Trade, sent a letter to Dmitri Alperovitch, Vice President of Threat Research at McAfee, requesting further information on his recently published report "Revealed: Operation Shady RAT."

First of all I'd like to say straight out that we do not share the concerns surrounding the intrusion described in the report, which intrusion the report claims has resulted in the theft of sensitive information of multiple governments, corporations and non-profit organizations.

We conducted detailed analysis of the Shady RAT botnet and its related malware, and can conclude that the reality of the matter (especially the technical specifics) differs greatly from the conclusions made by Mr. Alperovitch.

We consider those conclusions to be largely unfounded and not a good measure of the real threat level. Also, we cannot concede that the McAfee analyst was not aware of the groundlessness of the conclusions, leading us to being able to flag the report as alarmist due to its deliberately spreading misrepresented information.

I'd like to give my own answers to the key questions posed in the letter, to firmly

sophisticated nor novel. How do these unsophisticated intrusions differ from the intrusions that were the focus of your report?

Many of the so-called "unsophisticated" intrusions that the IT security industry has discovered recently and which have been so prominent in the news should in fact be labeled just the opposite: "sophisticated".

These sophisticated threats – such as TDSS, Zeus, Conficker, Bredolab, Stuxnet, Sinowal and Rustock – pose a much greater risk to governments, corporations and non-profit organizations than Shady RAT.

For example, TDSS controls one of the world's largest zombie networks, made up of more than 4.5 million computers worldwide. It contains extremely sophisticated techniques and implements a whole range of risky payloads that can lead to the theft of sensitive information and even funds in bank accounts, to spam distribution, DDoS attacks and much more.

On the other hand, most security vendors did not even bother assigning a name to Shady RAT's malware family, due to its being rather primitive.

Are such intrusions something the government and private sector can effectively prevent or mitigate on a continuing basis?

Most commercially-available anti-virus software is capable of preventing infection by the malware involved in Operation Shady RAT; most doesn't require a special update to do so either, capable of detecting the malware generically.

Did the logs analyzed by McAfee reveal novel techniques or patterns that would be helpful in our efforts to combat cybercrime?

We are fairly sure that the logs that McAfee analyzed did not differ from the logs all the other security vendors analyzed.

Here are our findings: unlike malware from the abovementioned sophisticated samples, we found no novel techniques or patterns used in this malware. What we did find were striking shortcomings that reveal the authors' low level of programming skill and lack of basic web security knowledge.

In addition, the way the malware spread – via masses of spam messages with infected files attached – is now considered to be old hat; most modern malware uses web attacks to get to target computers. Shady RAT also never used any advanced or previously unknown technologies for hiding itself in the system, any countermeasures against anti-viruses, or any encryption to protect the traffic between the servers and infected computers. Needless to say, these are features

information, or consumer information that can be used to perpetrate identity theft?

There is no evidence showing what sort of data has been acquired from infected computers, or if any data has been acquired at all.

We can only understand what data (if any) has been stolen by conducting an in-depth investigation within an affected organization to examine the actual access rights of the infected computers.

The report suggests that the more insidious intrusions are more likely to occur without public disclosure. Would more public disclosure help or harm industry efforts to fight this type of cybercrime?

Some of the more insidious intrusions take place without the general public becoming aware of them. What's more, they can go undetected for some time before being discovered by the IT security industry, and this is likely to continue due to the nature of the architecture of modern software and the Internet.

However, regarding Shady RAT, the IT security industry *did* know about this botnet, but decided not to ring any alarm bells due to its very low proliferation – as confirmed by our cloud-based cyber-threat monitoring system and by other security vendors. It has never been on the list of the most widespread threats.

For years now the industry has adopted the simple and helpful rule of not crying wolf.

A very important question that has slipped off the radar is what state is behind this intrusion?

It's not possible to give a straight and clear answer to this question; however, it looks overwhelmingly likely that no state is behind the Shady RAT botnet. How the botnet operates and the way the related malware is designed reveals startling fundamental defects hardly indicative of a well-funded cyber-attack backed up by a nation state.

A good example of a cyber-attack most likely backed by a nation state is Stuxnet. Just compare the number of vulnerabilities used, special techniques, and the various assessments of the development cost. With Shady RAT we are dealing with a lame piece of homebrew code that could have been written by a beginner.

On the black market the Shady RAT malware would be valued at not much more than a couple hundred dollars. Even if an "evil" state were to decide to launch a targeted attack, it could buy much more sophisticated malware for just $2,000

in-depth analysis of the botnet.

We believe that this act was performed by rather novice criminals who were testing the ground, but who didn't improve their skills much at all since the date they started the botnet.

To summarize the Shady RAT report:

Was it the most sophisticated attack ever?

No.

Was it the longest-lasting attack ever?

No.

Was it a historically unprecedented transfer of wealth?

No.

Is there proof that 71 organizations were compromised and had data leaked?

No.

Was it backed up by a state?

No.

Does Shady RAT deserve much attention?

No.

Useful link: Comment from Alex Gostev, Kaspersky Lab's Chief Security Expert

this real, uncertainty and doubt (FUD) is just to sell more products that do not work and especially maybe get a US government contract to sell the US govt “protection”

1 REPLY TO CONVERSATION

Anonymous

Guess you missed the recent show on China’s government run CCTV 7, “Military Technology: Internet storm is coming” that showed camera footage of Chinese government systems launching attacks against a U.S. target?

0 REPLY TO CONVERSATION

e_kaspersky

Oh no I didn’t. Did you saw an evidence they launched Shady RAT?

1 REPLY TO CONVERSATION

Adrian

Thanks very much for your analyses. Witnessing events unfold politically here in North America it’s concerning that the pattern of shoddy work you detail here with respect to “Shady RAT” is mirrored in elements of reporting we see on what the press has labelled the “hack” of the recent US election.

1 REPLY TO CONVERSATION

Trackbacks 24

Kaspersky disputes McAfee's Shady Rat report | TechRepublic

Read track

Kaspersky says McAfee report is all bark and no bite | National Cyber Security

Read track

Eugene Kaspersky juge le rapport Shady RAT de McAfee "infondé" | Exanders.fr

Read track

McAfee miente sobre Shady Rat, acusa CEO de Kaspersky | bSecure

Read track

Acusa CEO de Kaspersky a McAffe de mentir sobre operación Shady Rat | Netmedia.info ›

Read track
SECURITY FIRMS KNOCK HEADS OVER SHADY RAT HACKS » KASPERSKY, MCAFEE, MCAFEES, SHADY, SCHNECK, COMPUTERWORLD » GADGETTECHNEWS.CO.CC

Read track
Shady RAT… Shoddy RAT… What about “Shouty RATT” | SecurityCurve

Read track
Security firms knock heads over Shady RAT hacks | National Cyber Security

Read track
Security firms knock heads over Shady RAT hacks « Linux News « 123linux tutorials

Read track
Security firms knock heads over Shady RAT hacks | Stop Spam Tips

Read track
Security firms knock heads over Shady RAT hacks | LocatePC | Locate your stolen computer or stolen laptop – Works for both Mac and PC

Read track
Hacker Smack Talk Escalates | National Cyber Security

Read track
HACKER SMACK TALK ESCALATES » BART, GARCIA, ANTISEC, MCAFEE, SHIONOGI, SHADY » TECH MAGAZINE

Read track
Hacker Smack Talk Escalates | eTechwar

Read track
McAfee Defends Its Position on Operation Shady RAT | WebProNews

Read track
August 2011 Cyber Attacks Timeline (Part I) « Il Blog di Paolo Passeri

Read track
The Culture of “Cyber” Minimizes Effective Data Sharing

Read track
August 2011 Cyber Attacks Timeline « Il Blog di Paolo Passeri

Read track
Malware in august: un an de la primul troian care ataca platforma de operare Android. Top virusi/malware | Devirusare.com

Read track
Rooting out Rootkits. | Nota Bene

Read track
McAfee Blew Shady RAT Analysis | Information Security Consultants | NCX Group

Read track
Your APT can be a Botnet, and vice versa | Seculert Blog on Advanced Persistent Threats

MAY 17, 2018

THE NORTHERNMOST TOWN IN THE WORLD.

Hi folks! Ok, you've had your fun and games, now for some detail on my recent North Pole trip… Now, unlike some, I wasn't skiing to the North Pole. I consider myself sporty and adventurous… but I know my limits). No, I was going the lazy man's route: Oslo > Longyearbyen, Svalbard > Barneo […]

MAY 17, 2018

ARCTIC OR ANTARCTIC?… THE ANSWERS.

Hi folks! As promised, herewith, my answers to Thursday's polar quiz questions: Ok, first – my answers to those four non-visual questions: Question 1: How do you get to the North Pole? Answer A: The simplest and cheapest method: Buy a plane ticket from Dubai to Seattle or San Francisco. These routes fly real close […]

MAY 10, 2018

PHOTO-QUIZ: WHERE WERE THESE PICS TAKEN – THE ARCTIC OR ANTARCTICA?

Hi Folks! As promised, herewith, a rewind back to all things polar… – but with a twist. It's not a full-on description of what I was doing recently up at the North Pole, or why; that, I'm sure (if I do ever get some free time, finally!) will come later. No, this post is a bit […]

MAY 8, 2018

POLAR-TROPICAL CONTRASTS.

Hi boys and girls! Been a while, I know, but I'm back – and with loads of on-the-road tales to recount that have piled up… Right now I'm in Terminal 5 of Heathrow Airport, which is fitting: I've seen a lot of airport terminals just recently, but I haven't had enough time in the departures […]

APRIL 28, 2018

HAPPY WORLD IP DAY!

April 26: significant for you? Perhaps it's your birthday? If not, I bet you're a patent lawyer, or someone who works with patent lawyers. For April 26 is World Intellectual Property Day! Accordingly, yesterday I congratulated all those connected with this tricky profession, and wished them every success within it. Actually, not all those connected […]

APRIL 23, 2018

VANUATU DREAMIN'.

Throughout human history there have been many interesting moments and fascinating stories. Out of all of them, I reckon one of the most amazing is the story about how homo sapiens settled on remote islands across the Pacific. Around two or three thousand years ago, from the shores of what is today Papua New Guinea, […]

MORE

SEARCH

SITE MAP

PRIVACY POLICY

SEND US A SPECIFIC VIRUS

TAGS

.

BUZZ

EVENTS

SECURITY MATTERS

TRAVEL NOTES

GET SOCIAL