VITO LETTER ON SHADY RAT

Subject Line: Operation Shady RAT Shows History of 5 Years of Advanced Persistent Threats Against Over 70 Companies Worldwide

Dear <NAME>,

McAfee Labs, our premier research facilities, constantly monitor the worldwide threat situation. Recently they were able to gain access to the history logs of a command and control server (C&C) and review 5 years of attacks made by the server. We have nicknamed this server, Shady RAT (Remote Access Tool). Among the key findings:

- Every geography is targeted
- Every *type* of business (public, private, government) is targeted
- Every *size* of business (government agencies down to non-profits) is targeted
- APTs (Advanced Persistent Threats) are long-lived and relentless: the longest in this attack was 28 months (the average of 72 companies identified was 8.75 months)
- Stolen data now reaches into PETABYTES of content … that we know about
- We don't know where all of that information has gone, who has accessed it or what they have done with it

The fact is, **APTs hide in plain sight.** They avoid detection by using common network ports, process injection and Windows service persistence. APTs generally only initiate outbound network connections. So, unless an enterprise network is specifically monitoring outbound network traffic for APT-related anomalies, it will not identify the APT malware outbound beaconing attempts. The 70+ companies targeted by Shady RAT found this out the hard way.

One of the most interesting conclusions from our research team is:

> *"In the Fortune Global 2000, there are only 2 types of companies: those who have been attacked and KNOW it, and those who have been attacked and DON'T KNOW IT YET."*

<NAME>, I'd like to offer you a 30-minute executive briefing to discuss how you can block these types of attacks and not become a statistic. I promise this will be a great use of your time.

Kind Regards,

<insert your name and title>

direct <insert your number>

P.S. I will call you <insert date and time> to discuss in more detail. If this is not a good time, please contact me to schedule a more convenient time.