

# The Relevance of Shady RAT

Andrew Ginter

Like 1

0

3



Guest Blogger Andrew Ginter is the Director of Industrial Security for [Waterfall Security Solutions](#).

McAfee's **announcement last week** that it had taken over the command and control center for an advanced persistent threat (APT) dubbed "Shady RAT" got a lot of press. Now — before the nay-sayers jump on me, let's set the record straight: **no** — there was no indication in the McAfee report that control systems were targeted by this adversary. And you can say that to yourself over and over if it makes you feel less vulnerable.

The Shady RAT report provides valuable insight into advanced threats. The "APT" term has been over-used recently — it originally referred to what appeared to be nation-state intelligence agencies using cyber assaults for both conventional espionage and industrial espionage. The McAfee report uses the APT term in this original meaning.

Advanced threats have targeted control systems in the past. Earlier this year McAfee **reported "Night Dragon" attacks** on a half dozen large oil companies and reported that the attacks had stolen information from SCADA system as well as carrying out more conventional industrial espionage on corporate networks. The Stuxnet attack has widely been reported as an attack by an advanced threat as well, though the Stuxnet technology was much more sophisticated than is normally attributed to threats such as those behind Shady RAT and Night Dragon. People responsible for industrial control system security should be aware of advanced persistent threats, their capabilities, their targets, and their tactics.

The Shady RAT report is thin on technical detail and at 14 pages with lots of diagrams rates as fairly light reading — I recommend the entire report to everyone even somewhat interested in the topic. The report can be summarized:

- 72 organizations were compromised over 6 years.
- The attacks spanned many sectors, including governments, non-profits, heavy industry, technology companies and the defense industry.
- The targets spanned many geographies: 53 in North American, and 19 were spread out through Europe, India and Asia.

Perhaps the most important finding is that this looks like "the tip of the iceberg." McAfee reports having investigated many enterprises compromised by advanced threats, and only a few of those investigations correlate with this list of targets. This and other indications suggest that many other command and control centers exist, each with a comparable list of compromised targets. The problem really is widespread.

The report also confirms what has been reported as a favourite tactic of these advanced threats: remote access tools — hence the "RAT" moniker. Remote access tools have a look and feel comparable to the Windows "remote desktop" tool. You can see the screen of a compromised machine, move the mouse, and type on the keyboard. "SCADA" assets compromised this way provide an adversary, on the other side of the planet, remote control of equipment on your operations network.

There are technologies available which can help. There are no silver bullets, but one lesson we should take from advanced adversaries is that conventional "best practices" — firewalls, patching, anti-virus, and host hardening — are not enough and are not working. Operations security professionals need to start investigating technologies which are being added to the list of best practices in guidelines and standards:

- unidirectional gateways, which can block remote access attacks completely,
- whitelisting, which is harder to evade than are AV technologies,
- intrusion detection / SIEM, which let you assume you have been compromised and start looking for your adversaries,
- device firewalls, which limit damage when a control system is compromised, and
- strong authentication for I/O device communications, which, again, limit damage when a control system is compromised.

Yes — compared with corporate intrusions, we have only a small number of advanced attacks which are well-documented in the control system world. *But* — telling ourselves this means there is no risk is sticking our heads in the sand.

Image by [Charles Jeffrey Danoff](#)

12 August 2011 | Tags: [McAfee](#), [Shady Rat](#), [\[APT\]](#) | Category: [McAfee](#), [Research](#), [Vulnerabilities](#) | [2 comments](#)

## 2 comments to The Relevance of Shady RAT

**[Ralph Langner](#)**

12 Aug 2011 at 08:45

Thanks Andrew. Over here we also see a high relevance of Shady RAT. One issue that concerns me is the increase of targeted attacks. It looks like few people in operations and maintenance are aware that simply by opening an attachment that comes with a seemingly legitimate email can get your system compromised. The advice that we add to your bullet points is, no email clients in the process network. If you think you cannot do without email, use a client that runs in a different VLAN.

**[Andrew Ginter](#)**

12 Aug 2011 at 10:38

Thanks for the comment Ralph, and I agree.

Rather than a VLAN though, I prefer to see a corporate desktop machine connected to the corporate network, but physically available at operator and engineering desks/workstations. In my experience there are too many ways to mess up VLAN installation / maintenance and wind up much less secure than you thought you were.