OPINION

Ira Winkler: Shady Rat Case Shows Vendors As Big a Problem As APT Itself

Security vendors seem more focused on fighting each other than protecting their customers.

By Ira Winkler
Contributing Columnist, Computerworld
AUG 11, 2011 8:00 AM PT

McAfee reports a hack of unprecedented proportions , an attack referred to as an "advanced persistent threat" (APT), which potentially involved dozens of companies and organizations.

McAfee is then accused of trying to drum up business for its security services, and its competitors question whether this attack was really all that severe .

And I'm left wondering whether everyone isn't missing the point.

More on IT security:

- 5 information security threats that will dominate 2018
- 10 critical security skills every IT team needs
- How to measure cybersecurity effectiveness — before it's too late
- 10 ways you're failing at IT audits
- The CSO IoT security basics survival guide

It's hardly news that vendors overstate the importance of their studies. But if what is being referred to as Operation Shady Rat isn't the worst, the biggest or the most damaging hack in history, the fact remains that APT is a chronic problem affecting organizations around the world. And when APT is involved, there are no minor attacks.

But instead of acknowledging that it's a serious matter that such attacks are, indeed, a chronic problem, Symantec treats that as a big yawn.

"While this attack is indeed significant, it is one of many similar attacks taking place daily," said Symantec researcher Hon Lau. "Even as we speak, there are other malware groups targeting many other organizations in a similar manner in order to gain entry and pilfer secrets."

Lau's point seems to be that McAfee shouldn't be trying to cause a stir with its report, because what it's reporting is nothing new, and that McAfee is no more on top of the APT situation than Symantec.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from Pl

Meanwhile, Kaspersky stated that calling Shady Rat the "biggest attack is premature" when McAfee has provided very little inf
wants to see the details of what was compromised before it publicly entertains the notion. This is disingenuous. Kaspersky kn
uncovering a major breach, would hand the investigation over to law enforcement. Assuming that's what McAfee has done, th
could compromise that investigation.

Most laughable is the Symantec line of attack that tries to puncture the seriousness of Shady Rat by questioning whether it constituted an APT.

"Is the attack described in Operation Shady RAT a truly advanced persistent threat?" asked Lau. He then calls the attackers sloppy, noting that they left their own command-and-control servers open to probing and used "relatively non-sophisticated malware and techniques."

This is a prime example of missing the point. Do Lau and Symantec not realize that "APT" is just a moniker, and not a definition of the attacks? The word "advanced" is not meant to imply that every element of the attack is state of the art, but only that a high level of resources and coordination is exhibited in the attacks. Whether the hackers achieved their goals through advanced techniques or were in fact sloppy is beside the point; they do seem to have achieved their goals. Likewise, if Lau has an issue with an APT server being hacked, all he has to do is remember Shawn Carpenter, the network security analyst at Sandia National Laboratories who five years back was the first publicly confirmed APT anti-hacker after hacking a variety of APT servers to uncover a treasure trove of counterintelligence.

Maybe Symantec would feel better if we just changed the moniker "APT" to "Fred." Then, from my experience in investigating several Fred types of attacks, I could list these shared aspects of Fred attacks and not worry about Symantec saying some of it doesn't sound all that advanced:

1. The attackers appear to perform detailed reconnaissance on their target, developing pretexts for spearphishing attacks aimed at specific employees. The reconnaissance can be as deep as identifying co-workers, bosses, professional society memberships, business relationships, etc., and likely involves the use of information from LinkedIn profiles, 411.com and similar sites. 2. 3. The spearphishing messages are fairly basic, but typically contain a zero day, or near zero day, exploit that is highly customized to the target's technical environment.

4. A successful spearphishing attack downloads additional malware, and a team of people then uses the compromised system as a launch point to embed significantly more advanced malware throughout the network. The initial foothold can then be abandoned.

5. Typically, the attackers target the computers involved in the command, control and communications of the organization. This could include the PCs of C-level executives, critical network and database servers and email, VoIP and BlackBerry Enterprise Servers.

5. The malware tends to be extremely advanced in that it is composed of many small components that are encrypted and embedded across the network and that check for network or system state before launching in full mode. The full malware typically includes the establishment of covert channels for the malware's own command and control. Data exfiltration can occur over extended periods of time, as targeted data is located throughout the targeted organization.

No, you don't need to use supersophisticated techniques for a spearphishing attack -- just sophisticated enough. The major advanced aspect of APT attacks is the technical sophistication of the malware that is embedded in an organization, and not the malware used to establish the temporary foothold.

None of this is meant to refute the charge that the McAfee report was more about marketing than it was about releasing information. McAfee provided few details about the attack, only saying that it was large and hinting at who the targets were. There have been documented cases of state-sponsored hacking out of China for more than a decade, targeting every conceivable type of commercial and government organization. When you get down to it, McAfee seems to have collected information from a single server involved in such collection, and there are likely dozens, if not hundreds, of such servers. Far more information about this sort of thing came out in 2009, when The US-China Economic and Security Review Commission released a Northrop Grumman-prepared report called "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" . That paper is infinitely more informative than anything that any security company has been willing to disclose.

Which brings me to one of the most shameful aspects of the back and forth over Shady Rat. Symantec, in criticizing the McAfee report, provided basic details about how the attacks were accomplished and some information about how to filter out such attacks. Symantec's point again seems to be that all of this is old news. But the question for me is why it hasn't provided all of this information sooner. Why pull it out only after waiting for an opportunity to try to make the competition look bad?

This is the root of the problem with how security vendors are dealing with the chronic issue of APT. They treat their customers' misery as their own intellectual property. Companies that investigate APT-related attacks rarely share their findings. They don't exchange information about the most recent malware obfuscation techniques, the best methods to identify compromised systems, the newest malware signatures, etc. Instead, they keep most of the information to themselves and treat it as a competitive advantage. What sharing there is falls far short of what would be required to encourage a robust response capability.

Meanwhile, the FBI remains equally close-mouthed. A U.S. organization that falls victim to an APT probably won't know it until it receives a call from the FBI, which cryptically says that the FBI has been made aware that the organization has been sending out some corrupted DNS or other data to a suspicious server. The FBI tells them that they might want to look into that, and that's it.

My suggestion: Security companies and the FBI should get together and have a formal and meaningful exchange of information about the real malware involved in the Shady Rat operation, as well as the most effective techniques in identifying and mitigating APT compromises. Because when security companies treat their investigative findings as proprietary information, they leave everyone else to reinvent the malware mitigation wheel. This only helps APT attackers -- and of course the consultants in the unnecessary inflation of their invoices.

Ira Winkler is president of Internet Security Advisors Group and author of the book Spies Among Us. He can be contacted through his Web site, irawinkler.com .

Read more about security in Computerworld's Security Topic Center.

This story, "Ira Winkler: Shady Rat Case Shows Vendors As Big a Problem As APT Itself" was originally published by Computerworld.

Next read this:

- *9 forces shaping the future of IT*
- *How to break the CIO mold — and become a business leader*
- *7 habits of highly effective digital transformations*
- *The secrets of highly successful data analytics teams*
- *The best ERP systems: 10 enterprise resource planning tools compared*
- *Hidden cloud migration gotchas — and how to avoid them*
- *IT Resume Makeover: Highlighting transformational leadership*
- *10 old-school IT principles that still rule*

Ira Winkler, CISSP, is president of Secure Mentem, and author of the forthcoming book, Advanced Persistent Security. He can be contacted at securementem.com.

Follow