NOMURA
Beyond the world headlines: How is the sun still rising in Japan?

Welcome Back Symantec

OCT 27, 2015 @ 12:01 AM 5,059 VIEWS

Richard Stiennon
CONTRIBUTOR
I write about the IT security industry.
FOLLOW ON FORBES (60)

Opinions expressed by Forbes Contributors are their own.

FULL BIO

Beyond the world headlines: How is the sun still rising in Japan?
NOMURA
#nomuraconnects
Explore more at: www.nomura.com/connects ▶

It has been a long road but it appears that Symantec has finally re-focused on its core business of securing its customers. Symantec announced today that it is introducing an automated malware analysis and response solution, Symantec Advanced Threat Protection (ATP).

It has been 12 years since I first heard complaints from enterprises that their anti-virus solution was not detecting targeted malware, that is, malware that was customized just so it would *not* be detected by signature systems of the day. AV clients have been augmented over the years to include white-listing and behavior based technology. But still, they cannot keep up with the level of customization that targeted malware exhibits.

Beyond the world headlines: How is the sun still rising in Japan?
NOMURA
#nomuraconnects
Explore more at:
www.nomura.com/connects ▶

One approach that FireEye can lay claim to pioneering is sand boxing. Incoming malware, usually in email attachments are shunted to a virtual machine where they are allowed to execute, install, and beacon home. That behavior is monitored and used to extract key indicators of compromise (IoCs) which can then be used to further inform other diagnostic and protective tools. This is what Symantec ATP does.

As of this January Symantec will have divested itself of Veritas, the data center solution vendor it squandered its capital on in 2004. As a pure play security vendor once again, it has some catching up to do. Introducing an advanced malware defense to compete with FireEye, LastLine, and Trend Micro Systems, is exactly the right first step. Doing it with internal resources is also the right approach. An acquisition may have been considered but malware defense is Symantec's core business. This new solution is merely the productization of what Symantec already does, as do all AV vendors, in its automated research to discover new versions of malware and write signatures.

Symantec ATP includes Symantec Cynic, a new cloud-based sandboxing and payload detonation service. The scale offered by a cloud solution means that a customer's OS and standard applications like Adobe, and Microsoft Office can be emulated quickly and will have a higher catch rate of targeted malware. ATP also includes Synapse which is a cross-platform correlation tool that will be able to provide intelligence on infections.

This is great news for existing Symantec customers and dire news for FireEye which will have to compete on effectiveness, speed, ease of deployment, and price. It is also bad news for attackers who will have to invest much more in devising ways to bypass Symantec ATP.

See my latest book, There Will Be Cyberwar, and follow me on Twitter.

Comment on this story

Report Corrections Reprints & Permissions