[redacted]

From: Horst Joepen
To: Martin Stecher; Gary Taggart; Thomas Friedrich; Christian Matzen; Jobst Heinemann; Cyntia Sucher (E-Mail); Peter Borgolte; Michael Wittig (E-Mail)
CC:
BCC:
Sent Date: 2004-06-18 15:51:22:000
Received Date: 2004-06-18 15:51:23:000
Subject: Straw man / Draft Press Release to announce Proactive Security Feature
Attachments:

All,

looks like it needed the more quiet Friday afternoon hours to get =omething done ... please find below my first shot on the "Finjan =iller" press release.

Mike, I think you have been in the loop and had some discussions about =t with Martin. Cynthia, we can talk on Monday to give you some more =ackground on the subject.

Intend of the release is to unleash some deals that Finjan still is =talling by their product announcements and promises to customers, while =e have no official statement about our new proactive technology out =et. As our credibility with customers is much higher than Finjan's =they announced a SSL Scanner more than one year ago, but still did not =eliver), we can expect that this is sufficient to pull in several =arger deals in which we currently compete against Finjan.

Also, as there are new major announcements from other Cyberguard =nits/products, it might well serve to bridge the dry zone in which we =ack other good news. It would be great to get it out before end of =une.

As always, no pride of authorship - any feedback welcome.

Regards

Horst

EXHIBIT
36
GERMANY
PENGAD 800-631-6989

--=-----------

CyberGuard announces new WebWasher product to protect against Day Zero =irus attacks

Fort Lauderdale, June xxxx, 2004:

CyberGuard today announced a new product version, developed by its =ecently acquired Webwasher Content Security Management division, that =ill contain a new proactive protection technology against Viruses and =orms. It does not rely on classic Anti Virus patterns. In contrast to =urrently known behavioural Anti Virus technologies, CyberGuard's new

Plaintiff's Trial Exhibit
PTX-36
Case No. 06-369 GMS

[redacted]

=echnology offers up to 10 times higher detection rates, combined with =ubstantially reduced false positives, resulting from a combination of =nique new algorithms.

As patterns against new viruses by nature only can be developed and made =vailable by Anti Virus vendors within several hours after a new virus =as been detected, proactive technologies analyze Web and Email traffic =nd look for certain anomalities, objects or combination of objects and =ode. The technology is meant not to substitute conventional Anti Virus =echnology, but rather to complement it to maximize protection and =erformance - the proactive scanner does not need to look for a known =irus that can be caught faster by the pattern based scanner. It kicks =n behind the conventional scanner and only for those viruses, whose =attern are not yet known - the so called Day Zero attack. Higher =erformance also is achived by avoiding emulation of actual code like in =echnologies commonly known as "Sandboxing".

"There has been a lot of hype and disappointed expectations about =o-called Sandbox-technologies, that typically have only 90% detection =ates, along with 10% false positives. With CyberGuard's new technology, =e think the times of playing with toys in the sandbox are over - with a =ew virus or worm almost every day people want to have real solutions =hat do what they are supposed to do - catching unknown blended threads, =iruses and worms. And this solutions needs to be scalable, robust and =igh-performance, because you don't want increased security needs throw =ou back to the times when loading a Web page took several seconds - =owest latency is absolutely critical for filtering of Web traffic that =eeds to be displayed in the browser in real time." said xxxxxx, xxxxxx =t CyberGuard's Webwasher division.

"Analyst Quote?" - we can do a briefing call with Brian Burke, using =artin's slide set...

WebWasher by CyberGuard provides leading Content Security technology =hat integrates URL Filtering, Web and Email AntiVirus, Anti Spam, =M/P2P Filtering and Reporting in one product suite.

The new function will be part of Webwasher AntiVirus Version 5.2 and =ebwasher CSM Suite Version 5.2, which will become available in October, =t no additional cost - the current pricing of Webwasher AntiVirus will =emain unchanged. All customers purchasing WebWasher AntiVirus or =ebwasher CSM between now and availability of the new version will =eceive a free upgrade.

<Boiler plate: about CyberGuard>

> -----Ursprüngliche Nachricht-----
> Von: Martin Stecher
> Gesendet: Dienstag, 1. Juni 2004 11:30
> An: 'mwittig@cyberguard.com'; Gary Taggart; Thomas Friedrich;
> Christian
> Matzen; Horst Joepen; Jobst Heinemann
> Cc: Peter Borgolte; Martin Stecher
> Betreff: Proactive Security Feature Direction
>
>
> Hi,
>

[redacted]

> on Friday we (some techies) met to talk about ways to
> implement the Proactive Security Feature (a.k.a. the Finjan
> Killer) for WW 5.1.
>
> We found basically two fundamentally different approaches.
> Please have a look which of these does better meet corporate
> policy and sales desire. We need your input and a decision
> soon. It is not a technical question but only sales and
> marketing that should decide where we go here.
>
> If I could get your comments until end of this week? Would be great.
>
>
> We will need to write a scanner for JavaScripts, VB-Scripts,
> Java Applets, ActiveX Controls and other binaries. Adding a
> parser for VBA would outperform Finjan feature set as they do
> not scan Office documents at all.
>
> After the scan, WW must decide what to do with the file. Then
> we can do one of these options:
>
> 1. Look for potentially dangerous stuff within those files.
> The problem here is that the scanner can only check for some
> few criteria and there will be tons of bypass
> vulnerabilities; especially in binary code (such as in
> ActiveX controls) calls to dangerous functions can easily be
> overseen by the scanner. This option has a policy that the
> admin can modify to filter files.
>
> 2. Only allow those files for which a scanner can determine
> that it is harmless. This would only be a minority of files
> as scanning of for example Active X binaries is limited and
> the code would need to reject all files that call any unknown
> kernel function.
> For JavaScripts we could implement a parser that would
> execute some hard to parse function calls in a sandbox to
> verify the parameters making this.
> This option has no policy that can be set but a strict
> hardcoded definition what we believe is harmless.
>
> Option 1 is what Finjan does. Question is whether our (new)
> corporate policy allows us to follow this path. It pretends
> some deep level of security, which is actually not there. We
> would not feel comfortable with promoting this approach. On
> the other hand it is that what Finjan has and we would
> compete exactly with them. But it will also give us a hard
> time as we cannot expect that the first version will have the
> same number of filter settings and capabilities. They will
> also check very carefully which of their patents we may touch
> by recreating their system.
>

[redacted]

> Option 2 contains something like a real sandbox for
> JavaScript, which even Finjan does not have. On the other
> hand this technology may corrupt some web pages and may
> create many false positives, especially for the binary files,
> which the scanner cannot easily parse, more than 90% of the
> files could not be considered harmless.
> This would be the strategy of all customers that like to have
> a tight Internet policy but do not want to block everything,
> especially in the JavaScript context but could afford to
> block nearly all executables.
> In order to make it feasible we should add a fingerprint
> database in form of a subscription model that will allow us
> to continuously update a white list of files that we found to
> be harmless in our lab but found be detected as not harmless
> by the scanner. An automatic feedback function would allow
> the customer to send classified files to us for further
> investigations. This costs many additional resources in TPT.
>
> Estimated error rates:
>
> Option 1 Option 2
> Undetected malicious scripts ~10% ~1%
> Undetected malicious binaries ~30% ~5%
> Blocked harmless scripts ~10% ~10%
> Blocked harmless binaries ~10%
> ~90% (w/o database)
>
>
> Whatever option we choose or whether you wish to suggest an
> alternative way, this feature will cost a lot of resources.
> Surprise, surprise that a feature that Finjan works on for
> years cannot be done within a few weeks.
>
>
> Regards
> Martin
>
> --
> ____
>
> Martin Stecher
> Dipl.-Informatiker
> VP Development
>
> webwasher AG - a CyberGuard Company
> Vattmannstrasse 3
> 33100 Paderborn / Germany
>
> Phone: +49 52 51 / 5 00 54-25
> Fax: +49 52 51 / 5 00 54-11
> Mobile: +49 170 / 786 4700

[redacted]

```
> mailto:martin.stecher@webwasher.com
> Visit us at: http://www.webwasher.com
> http://www.cyberguard.com
> ____________________________________________
>
>
```

```
From IMCEAEX-_O=BWASHER-
MAIL_OU=RST+20ADMINISTRATIVE+20GROUP_CN=CIPIENTS_CN=RTIN+2ESTECHER@
Fri Jun 18 19:44:50 2004
X-MimeOLE: Produced By Microsoft Exchange V6.5
Received: by EMEA.scur.com
id <01C4555B.F4BA433F@EMEA.scur.com>; Fri, 18 Jun 2004 18:44:50 +0100
MIME-Version: 1.0
Content-Type: text/plain;
charset=so-8859-1"
Content-Transfer-Encoding: quoted-printable
Content-class: urn:content-classes:message
Subject: RE: Straw man / Draft Press Release to announce Proactive Security Feature
Date: Fri, 18 Jun 2004 18:44:50 +0100
Message-ID: <75F7E67FC45F6744A7D328D41E35376D13E0B6@mail.webwasher.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
Thread-Topic: Proactive Security Feature Direction
Thread-Index: AcRHuwzDri57Hp0aSzK12FYq+eD/1gL73zrAAGw3V2A=rom: "Martin Stecher"
<IMCEAEX-_O=BWASHER-
MAIL_OU=RST+20ADMINISTRATIVE+20GROUP_CN=CIPIENTS_CN=RTIN+2ESTECHER@
To: "Horst Joepen" <horst.joepen@WEBWASHER.com>
Cc: "Gary Taggart" <gary.taggart@WEBWASHER.com>,
"Thomas Friedrich" <thomas.friedrich@WEBWASHER.com>,
"Christian Matzen" <christian.matzen@WEBWASHER.com>,
"Jobst Heinemann" <jobst.heinemann@WEBWASHER.com>,
"Cyntia Sucher \(E-Mail\)" <csucher@mpbc.cc>,
"Peter Borgolte" <peter.borgolte@WEBWASHER.com>,
"Michael Wittig \(E-Mail\)" <mwittig@cyberguard.com>
X-Length: 12028
X-UID: 109
```

Horst,

so far we had been looking at these features to become part of the =Webwasher Content Protection" product not the "Webwasher Anti Virus" =roduct.
Especially if we add the library/database for known harmless files, we'd =ave the subscription model that we wanted to add to Content Protection.
If this could still be the strategy we may rethink the price of that =roduct.

Regards
Martin

```
> -----Ursprüngliche Nachricht-----
> Von: Horst Joepen
```

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**