



This week's sponsor: XQ cyber red teaming experts. Claim your free 1-day workshop and put your cyber defence team through its paces.

Zero-day vulnerabilities reportedly found in Kaspersky and FireEye security products

Graham Cluley | September 7, 2015 9:40 am | Filed under: **Google, Malware, Vulnerability** | 6



292



142



12



199

Sounds like it's going to be a busy few days for R&D and PR departments at least two security companies.



malicious hackers.



First up was Tavis Ormandy.

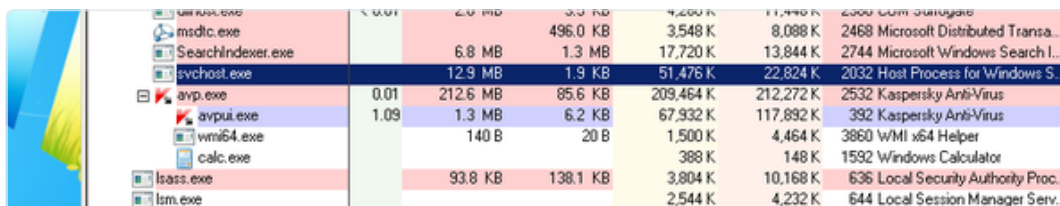
Ormandy, a security researcher at Google, has made a controversial name for himself over the years disclosing security vulnerabilities in products from other software vendors.

His critics, **of which I'm one**, fear that he has sometimes put innocent users at risk by not working on a co-ordinated disclosure with the manufacturer of the vulnerable software, ensuring that all users are protected with a patch before details of how to exploit the flaw are made public.



At the end of last week, Ormandy tweeted that he had successfully

exploited Kaspersky's anti-virus product in such a way that users could find their systems easily compromised by malicious hackers.



Process Name	Private Bytes	Working Set	Private Bytes	Working Set	Private Bytes	Working Set
smss.exe	2.0 MB	3.0 KB	4,200 K	11,440 K	2,000 K	3,000 K
msdtc.exe	496.0 KB	3,548 K	8,088 K	2468 Microsoft Distributed Transa...		
SearchIndexer.exe	6.8 MB	1.3 MB	17,720 K	13,844 K	2744 Microsoft Windows Search I...	
svchost.exe	12.9 MB	1.9 KB	51,476 K	22,824 K	2032 Host Process for Windows S...	
avp.exe	0.01	212.6 MB	85.6 KB	209,464 K	212,272 K	2532 Kaspersky Anti-Virus
avpui.exe	1.09	1.3 MB	6.2 KB	67,932 K	117,892 K	392 Kaspersky Anti-Virus
wmi64.exe		140 B	20 B	1,500 K	4,464 K	3860 WMI x64 Helper
calc.exe				388 K	148 K	1592 Windows Calculator
lsass.exe	93.8 KB	138.1 KB	3,804 K	10,168 K	636 Local Security Authority Proc...	
lsmon.exe			2,544 K	4,232 K	644 Local Session Manager Serv...	



Tavis Ormandy

@taviso

Follow

Okay, first Kaspersky exploit finished, works great on 15 and 16.
Will mail report after dinner. /cc @ryanaraine

10:43 AM - 5 Sep 2015

400

282

Ormandy has previously published details of how he has exploited anti-virus products from Sophos and ESET.

In a follow-up to his latest announcement, Ormandy tweeted that the flaw was "a remote, zero interaction SYSTEM exploit, in default config. So, about as bad as it gets."

One has to question the timing of Ormandy's announcement just before a long holiday weekend in the United States, which clearly makes it difficult as possible for a corporation to put together a response for concerned users. I supposed we should be grateful that he at least ensured that Ryan Naraine, a reporter at Kaspersky's Threatpost blog, was cc'd on the announcement.

None of this, of course, is to say that the vulnerability doesn't sound serious, and Kaspersky would be wise to investigate and fix it at the earliest opportunity. Ideally vulnerabilities should be found by a company's internal team, or ironed out before software ever gets released. And it's better that someone like Ormandy finds a flaw rather than a malicious hacking gang.

Nonetheless, one remains concerned that in the past malicious hackers have taken details of flaws published by Google's Tavis Ormandy, and used them in attacks.

Meanwhile, another security researcher had an important announcement this US holiday weekend, revealing that he had found flaws in FireEye's software.

As **CSO reports**, Kristian Erik Hermansen has disclosed details of a zero-day vulnerability, which - if exploited - can result in unauthorised file disclosure.



Regrettably, Hermansen published proof-of-concept code showing how the vulnerability could be triggered, and claimed that he had found three other vulnerabilities in FireEye's product. All are said to be up for sale.

"FireEye appliance, unauthorized remote root file system access. Oh cool, web server runs as root! Now that's excellent security from a `_security_` vendor :) Why would you trust these people to have this device on your network."

"Just one of many handfuls of FireEye / Mandiant Oday. Been sitting on this for more than 18 months with no fix from those security "experts" at FireEye. Pretty sure Mandiant staff coded this and other bugs into the products. Even more sad, FireEye has no external security researcher reporting process."

If you use products from Kaspersky or FireEye you may wish to contact their technical support departments to see if they can shed any more light on these issues. Be sure to be nice to them. Chances are they didn't have a great holiday weekend.

Update:

According to Ormandy, Kaspersky is rolling out a fix globally. That sounds like a great response from the Russian anti-virus firm.

**Tavis Ormandy**

@taviso

[Follow](#)

Kaspersky tell me they're rolling out a fix globally right now, that was less than 24hrs.

10:50 AM - 6 Sep 2015

39

34

Kaspersky has been in touch with an official statement:

"We would like to thank Mr. Tavis Ormandy for reporting to us a buffer overflow vulnerability, which our specialists fixed within 24 hours of its disclosure. A fix has already been distributed via automatic updates to all our clients and customers. We're improving our mitigation strategies to prevent exploiting of inherent imperfections of our software in the future. For instance, we already use such technologies as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP).

Kaspersky Lab has always supported the assessment of our solutions by independent researchers. Their ongoing efforts help us to make our solutions stronger, more productive and more reliable."



292



142



12



199

You might also like



Microsoft patches Windows, Internet Explorer and Office against funky font security flaws



Google says it will be (a little) less evil over vulnerability disclosure



'The Mask' malware campaign, undetected by anti-virus firms since 2007?



"Diskless" Internet Explorer zero-day attack discovered in the wild

Tags: **fireeye**, **kaspersky**, **kristian erik hermansen**, **malware**, **tavis ormandy**, **vulnerability**

Get GCHQ, Graham Cluley's unmissable security newsletter, delivered direct to your inbox. It's free!

Name

Email

GO!



About the author, Graham Cluley

Graham Cluley is a veteran of the anti-virus industry having worked for a number of security companies since the early 1990s when he wrote the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Now an independent security analyst, he regularly makes **media appearances** and gives **presentations** on the topic of computer security and online privacy. Follow him on Twitter at **@gcluley**, **Google Plus**, **Facebook**, or **drop him an email**.

[View all posts by Graham Cluley →](#)

Follow @gcluley 38.9K followers

< **Latvian pleads guilty in Gozi malware case that infected over a million PCs** [🔗](#)

Test yourself like the bad guys will... before they do.
[Sponsor] >

6 Responses



Martijn ⁽¹⁾ September 7, 2015 at 10:03 am <#>

REPLY [↩](#)

(Ryan works for Kaspersky itself, not for Threatpost.)

Although I don't think it's an excuse to offer bounties up for sale, it's worth noting that FireEye has allegedly threatened to sue researchers who reported vulnerabilities – for reasons that Oracle's MAD would probably approve of.

I do wish security vendors started to offer bug bounty programs, or at least treated vulnerability disclosure seriously.



David L ⁽⁴⁹⁾ September 7, 2015 at 10:09 pm <#>

REPLY [↩](#)

Hi,

I know for a fact that Avast does pay researchers for vulns, and after a guy named Korret discovered many AV mobile apps had vulnerabilities Avast willingly and gladly rewarded him a substantial amount of cash. I think it was between 5 & 6 figure. I believe the presentation was Blackhat 2014 Asia conference. Anyways, most of the AV vendors either ignored him, and or ridiculed and threatened him for his efforts. Typical of arrogant AV vendors like Fireeye! I will dig up the article. Stay tuned.



David L ⁽⁴⁹⁾ September 8, 2015 at 12:18 am #

REPLY ↩

Ok,here is the story from last years Syscan presentation about Korrets

findings.http://m.theregister.co.uk/2014/07/29/antivirus_blood_splattered_as_biz_warned_audit_or_die/

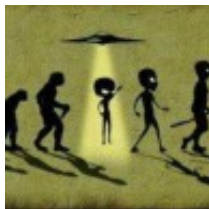
And this bit from pcworld about Kaspersky:

The issues in Kaspersky Lab's antivirus products that were outlined in Koret's presentation, namely the absence of ASLR in some components and a potential denial-of-service issue when scanning nested archives, are not critical to the security protection of the company's customers, a Kaspersky representative said via email. Software that is written without ASLR is not implicitly more vulnerable to exploits, but Kaspersky Lab added ASLR to the product components that were lacking it—vlins.kdl and avzkrnl.dll—after Koret's presentation, he said.

And check this out about over 30,000 apps in playstore with MALWARE:

http://www.theregister.co.uk/2015/08/31/massvet_finding_unknown_malice_in_10_seconds_mass_vetting_for_new_threats_at_the_googleplay_scale/

Tossed that in because it's not getting the attention it deserves,so please pass it along,thanks.



✓ **graphicequaliser** ⁽⁶⁾ September 7, 2015 at 2:36 pm #

REPLY ↩

disgusting!

And, consider, that FireEye's problem has been there for over 18 months and has still not been fixed, despite being in the public forum now. For a security product, that's

**Leftist** ⁽¹⁾ September 7, 2015 at 7:54 pm #

REPLY ↩

Not to mention that these vulnerabilities are _disturbingly_ simple.

A single run with AppScan or Zap would have found these flaws. This is laziness, lack of focus and incompetence at their worse.

Fireeye seems like a throwback to mid-2000's "security" vendors like Lumigent who made your systems markedly less secure by implementing them.

**Spennick** ⁽³⁾ September 7, 2015 at 5:32 pm #

REPLY ↩

Kudos to the folks at Kaspersky, first for hustling out a patch so quickly, and secondly for having way more professionalism and class than Mr. Ormandy has in irresponsibly disclosing the vulnerability on a zero-day basis.

For the record, I wouldn't dream of accusing "taviso" of being an arrogant, smirking little twerp who doesn't have the wits or character to discern the difference between notoriety and good reputation, so just put that thought out of your head right now. But the photo shown in the article does convey a certain...uh, shall we say "impression" of his attitude.

Leave a Reply

Name (required)

Email (will not be published) (required)

3000

 characters available

SUBMIT COMMENT

Reply notification?

Don't subscribe



Login

Username or
Email

Password

☐ Remember Me

LOG IN

[Register](#) | [Lost your password?](#)

Got a question?

Ask the forum!

Recent Questions & Answers



Can I backup and "wipe" or reset a
smartphone or tablet?

🕒 answered 3 hours ago



Can I backup and "wipe" or reset a smartphone or tablet?

answered 5 hours ago



Can I backup and "wipe" or reset a smartphone or tablet?

asked 10 hours ago



Why in 19 years hasn't a senior VP at Adobe realized flash is embarrassing?

answered 16 hours ago



Is there any way to use a password manager with bank websites?

answered 4 days ago

Public speaking



Hire Graham Cluley to speak at your event

Latest videos

The Internet of insecure Things | Graham Cluley

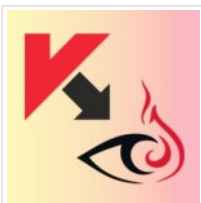
The POODLE bug! SSL vulnerability explained | Graham Cluley

[Visit Graham Cluley's YouTube channel](#)

LATEST POPULAR



Customers of UK's Metro Bank targeted by Twitter fraudsters [🔗](#)



Zero-day vulnerabilities reportedly found in Kaspersky and FireEye security products



Latvian pleads guilty in Gozi malware case that infected over a million PCs [🔗](#)



The 2015 Industrial Control Systems (ICS) Cyber Security Conference. Training and workshops included.

[Register today! \[Sponsor\]](#)

'Why I fell victim to a LinkedIn scam - and



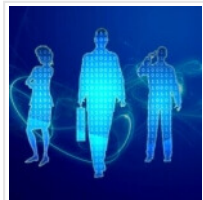
why I would do so again tomorrow'



How a simple email error revealed the identities of hundreds of HIV patients



If you look after the Large Hadron Collider you should read this...



Microsoft tracks Windows 7 and 8 users, harvesting more data



225,000 reasons not to jailbreak your iPhone - iOS malware in the wild [🔗](#)



Join me for a Mumsnet web chat



UK's National Crime Agency hit by DDoS attack, following LizardStresser arrests [🔗](#)

TalkTalk isn't helping customers use safer passwords



How can banana peels help the infosec community?



GhostMail. Encrypted email, chat & cloud storage. FREE and easy to use. [Sponsor]



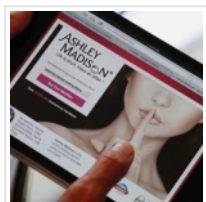
Ashley Madison's marketing department clearly didn't get the memo





Ashley Madison hack claims another victim: Its CEO

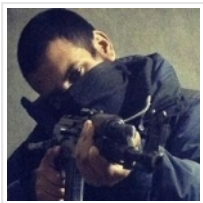


LizardStresser: Six people arrested in connection with Lizard Squad's DDoS attack tool



The Ashley Madison mystery: why would you use your work email address? 

Team Poison hacker believed killed by US drone strike 



Another nail in Adobe
Flash's coffin - Chrome to
block Flash ads from
September 1st

Categories

adobe (99) adobe flash (52) android (141) apple (315) apple safari (28) awards (6) blackberry (17) botnet (72) celebrities (121) clickjacking (32) data loss (671) denial of service (134) encryption (85) facebook (604) fake anti-virus (35) feed only (32) firefox (34) google (186) google chrome (21) google plus (4) guest blog (2837) hacked celebrities (49) internet explorer (54) ios (154) java (35) law & order (812) linkedin (22) linux (25) malware (1466) microsoft (211) mobile (223) naked security (75) nude celebrities (40) operating systems (1) oracle (21) os x (94) pdf (35) phishing (207) podcast (37) privacy (871) ransomware (31) rogue applications (85) security threats (61) social networks (696) spam (1071) sponsor (28) twitter (320) uncategorized (2) video (251) vulnerability (917) web browsers (44) windows (134) windows phone (9) yahoo (38)

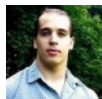
Contributors



Graham Cluley (3901)



Bob Covello (8)



David Bisson (8)



Lisa Vaas (3)



Per Thorsheim (3)

[More...](#)

Want to write for this site?

If you have an article that you'd like to share on grahamcluley.com, check out our [contributor guidelines](#).

Follow



Contact

[Send a tip or story idea](#)

[Hire Graham Cluley to speak at your event](#)

[Sponsorship](#)

[Complaints/Corrections](#)

[Privacy Policy](#)

[Contact Graham Cluley](#)

Copyright © 2015 Cluley Associates Limited. All Rights Reserved | [About](#) | [Cookies](#) | [Terms & Conditions](#)

Powered by [WordPress](#) | Hosted by [WP Engine](#)

This site uses cookies [That's fine](#) [More info](#)