June 2015
Feature Article: Professor Klaus Brunnstein

ENJOY SAFER TECHNOLOGY™

Table of Contents

Professor Klaus Brunnstein

David Harley, ESET Senior Research Fellow

[A version of this post originally appeared on the IT Security UK web site on May 21st 2015].

Like many others in the security industry, I was sad to hear of the death of Professor Dr. Klaus Brunnstein, who died on 20th May 2015, by my reckoning just a few days before his 78th birthday. His name won't mean much to most of my UK and US friends outside the security industry, though as ESET's Tommi Uhlemann suggested:

> *"In Germany he'll mostly be remembered for his fight for data protection in the 80's. He played a leading role in having new laws in this field".*

His political and academic activities went far wider than the anti-virus industry (as it was usually referred to then), but his direct contribution to the development of the security industry was in itself immense: it's particularly hard for us in the anti-malware industry to imagine what the industry would be like if it hadn't been for his wisdom and leadership. Graham Cluley commented:

> *"Klaus was an important and respected member of the anti-virus community, in particular during the 1990s when he ran the Virus Test Center at the University of Hamburg which was renowned for the quality of its tests, and helped produce some world-class experts who later benefited the industry".*

Marko Helenius has his own memories of Klaus's academic significance, and commented:

> *"Sad news, indeed. I have warm memories from the beautiful day when he was the opponent of my dissertation and our guest here in Tampere in June 2002".*

Professor Emeritus Pertti Järvinen of the University of Tampere adds:

> *"I worked with Prof. Klaus Brunnstein closely between 1990 and 1996 when he was a chairman of IFIP (International Federation of Information Processing) of TC9 (Technical Committee 9) Computers and Society and I was a secretary of TC9. He well managed all the affairs of TC9 and it was easy to write a minutes of TC9 meeting, because decisions were clear and well-formulated. I must only ask him more than once to check my draft. Klaus had already then too much work but he, however, succeeded nicely.*
>
> *Later I used Klaus' expertise as an opponent of Marko Helenius' doctoral dissertation (A System to Support the Analysis of Antivirus Products' Virus Detection Capabilities) and as a pre-examiner of Andro Kull's doctoral dissertation (A Method for*

Continuous Information Technology Supervision: The Case of the Estonian Financial Sector)".

Professor Järvinen's observations are a salutary reminder that Klaus's legacy also lives on in the academic research of those that worked with him, as well as in the industry-facing groups in which he was so influential. Andro Kull also commented subsequently:

> *"Even though I only interacted with him via e-mail, he gave me a strong confidence to pursue my doctoral work – thanks a lot for that. Rest in peace".*

James Wolfe, long associated with EICAR, AVIEN, CME and the WildList Organization, said:

> *"It's been a while since I saw Klaus face to face. He was incredibly smart but his intellect was tempered with patience and understanding. He always provided remarkable insight into most subjects and his input will be missed. He was a Founding Father for us in the industry. He was also an amazing educator. Every time I've taught at University, I've tried to model my teaching style on his. This is very sad…".*

Prof. S.C. Bhatnagar, honorary adjunct professor at the Indian Institute of Management, Ahmedabad, is founding chair of IFIP WG 9.4 on Social Implications of Computers in Developing Countries. He told me:

> *"Klaus Brunnstein was instrumental in the creation of the working group. He championed my proposal to create the group within the IFIP General Assembly. His heart was in the right place. He had never been to a developing country then, but he understood the special challenges faced by poorer countries in harnessing the power of ICT for development.*
>
> *He was a warm person and a gracious host who held some TC 9 meetings on his personal yacht.*
>
> *May his soul rest in peace".*

Seiji Murakami, long associated with AVAR (The Association of Anti Virus Asia Researchers) said:

> *"I would like to express my deepest condolences for prof. Brunnstein and his family.*
>
> *I appreciate his great help and support to me and to the development of antivirus industry in Asia in the early days".*

Anti-virus pioneer Dr. Alan Solomon observed:

> *"Very few people will know his leading role in establishing CARO and the cooperation between the technical people at AV companies so that everyone who needed access to a virus library could safely share, which improved all AV products".*

It had been hoped that he would be able to attend this year's CARO workshop, but ESET North America CEO Andrew Lee observed:

> *"Sadly missed, he wasn't able to make it to the CARO conference a couple of weeks ago. I only met him a few times, but it was always memorable".*

Although I only had the pleasure of meeting Klaus once in person, I communicated with him many times via email and worked with him on one or two EICAR projects, and like so many other people was struck by the depth and breadth of his knowledge and his unfailing helpfulness and courtesy. And I can also remember at the beginning of my career in security gathering a great deal of information about specific malware from the Virus Test Center. Luca Sambucci says:

> *"This saddens me so much. Klaus Brunnstein was the first person I got in contact with when I wanted to know more about computer viruses. It was I think 1990 and I was sixteen. I wrote him directly to his University and without much shame. He encouraged me to continue my research and I did so with enthusiasm. We stayed in touch for the next ten years or so".*

Virus Bulletin republished a 1996 interview with Klaus, in which he talked 'about his background, his career, his views and his home life.' There are many of us who'll remember him with gratitude. I'm so glad that I finally got the chance to shake his hand at a CARO meeting a few years ago. But I'll leave the last word to Aryeh Goretsky:

> *"We had corresponded numerous times over the years when I was at McAfee Associates, and I really appreciated how he took time out of his schedule to explain not just various technical minutiae to me, but also discussing how the field was evolving.*
>
> *I think it is sometimes hard to remember that the microcomputer security field is young enough that some of the people who pioneered it are still around. The passing of pioneers like Yisrael Radai, Harold Highland and now Klaus Brunnstein underscores the fragility and change of that, though".*

ESET Corporate News

Dino: new espionage malware from Animal Farm

ESET **has** published an in-depth research article entitled 'Dino - the latest spying malware from an allegedly French espionage group analysed'. ESET research found further evidence to suggest that this technically complex backdoor Trojan used for espionage purposes was coded by French speakers**. The malware was c**reated by the notorious Animal Farm espionage group - the team behind the sophisticated malicious attacks Casper, Bunny and Babar.

"Dino is basically an elaborate backdoor Trojan, built in a modular fashion," explains Joan Calvet, the ESET Malware Researcher who analysed the malware. "Among several technical innovations, there is a custom file system used to execute commands in a stealthy fashion as well as a complex task-scheduling module that works in a similar way to the 'cron' Unix command"**.**

ESET released beta version of ESET® Mail Security 6 for Microsoft Exchange

ESET announced the open Beta testing of ESET Mail Security 6 for Microsoft Exchange Server with a new user interface and even more layers of protection.

Other notable benefits of ESET Mail Security 6 for Microsoft Exchange Server Beta are:

- Servicing level priority – Provides higher flexibility when hot-fixing issues asssociated with the migration of Windows server products code to the most recent development stream.

- Added Layers of Protection – These include Advanced Memory Scanner, Exploit Blocker and Anti-Phishing. Find out more about these technologies on this ESET Technology page.

- ESET LiveGrid® – Reduces reaction time down to couple of minutes when attacks come in frequent waves, even without regular virus signature updates.

- Server-oriented usage patterns – All relevant logs that help to analyze server activity and are crucial for troubleshooting are now less than a click away from the main window.

The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 3.36%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL from which it tries to download several files. The files are then executed and HTTP is used for communication with the C&C to receive new commands. The worm may delete the following file extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

2. Win32/Adware.MultiPlug

Previous Ranking: 1
Percentage Detected: 2.71%

Win32/Adware.Multiplug is a Possible Unwanted Application that once it gets a foothold on the users system might cause applications to display pop-up advertising windows during internet browsing.

3. LNK/Agent.BO

Previous Ranking: N/A
Percentage Detected: 2.24%

LNK/Agent.BO is a link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.

4. JS/Kryptik.I

Previous Ranking: 3
Percentage Detected: 1.86%

JS/Kryptik is a generic detection of malicious obfuscated JavaScript code embedded in HTML pages; it usually redirects the browser to a malicious URL or implements a specific exploit.

5. LNK/Agent.AV

Previous Ranking: 4
Percentage Detected: 1.52%

LNK/Agent.AV is another link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.

6. Win32/AdWare.ConvertAd

Previous Ranking: 5
Percentage Detected: 1.48%

Win32/Adware.ConvertAd is an adware used for delivery of unsolicited advertisements. The adware is usually a component of other malware.

7. Win32/Sality

Previous Ranking: 6
Percentage Detected: 1.37%

Sality is a polymorphic file infector. When it is executed registry keys are created or deleted related to security applications in the system and to ensure that the malicious process restarts each time the operating system is rebooted.
It modifies EXE and SCR files and disables services and processes implemented by and associated with security solutions.

More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

8. Win32/Ramnit

Previous Ranking: 7
Percentage Detected: 1.26%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and also searches htm and html files so as to insert malicious instructions into them. It exploits a vulnerability (CVE-2010-2568) found on the system that allows it to execute arbitrary code. It can be controlled remotely to capture screenshots, send information it has gathered, download files from a remote computer and/or the Internet, and run executable files or shut down/restart the computer.

9. INF/Autorun

Previous Ranking: 8
Percentage Detected: 1.22%

INF/Autorun is a generic detection of multiple malicious versions of the autorun.inf configuration file created by malware. The malicious AUTORUN.INF file contains the path to the malware executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malware executable when the infected drive is mounted. The AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes present in an attempt to hide the file from Windows Explorer.

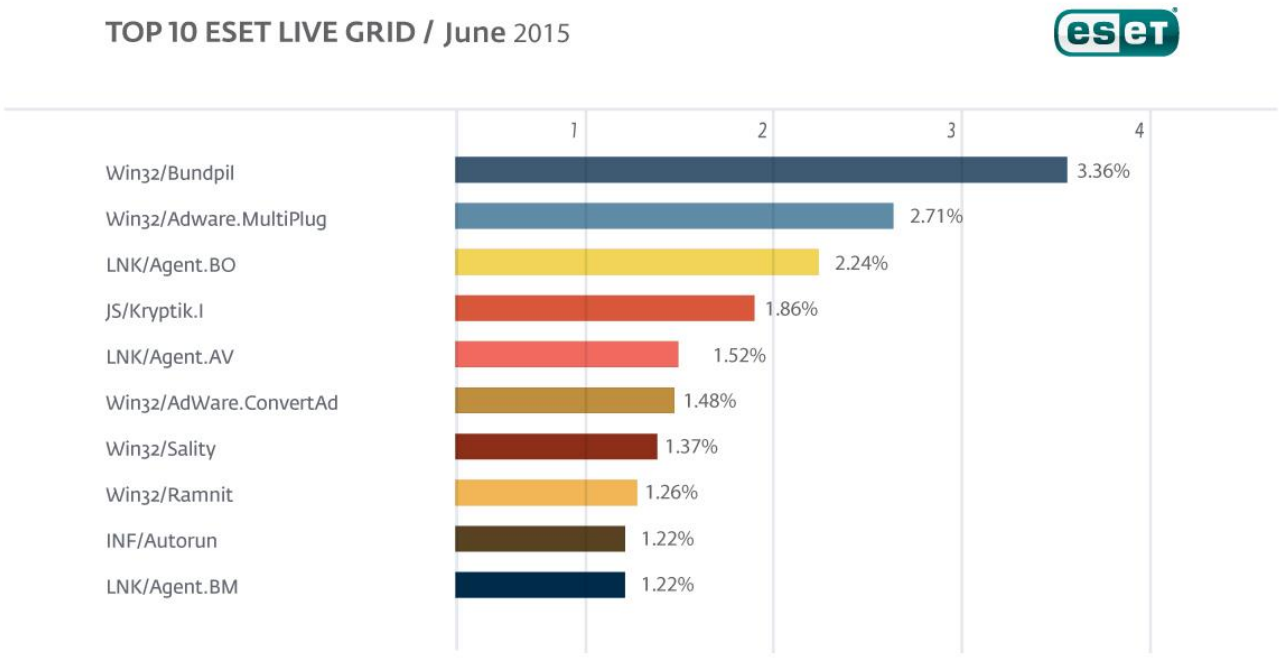
10. LNK/Agent.BM

Previous Ranking: N/A
Percentage Detected: 1.22%

LNK/Agent.BM is another link that concatenates commands to execute legitimate code while running the threat code in the background. It is similar in its effect to the older autorun.inf type of threat.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 3.36% of the total, was scored by the Win32/Bundpil class of treat.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- WeLiveSecurity
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation