# Threat Radar

## November 2017
## Feature Article: Antimalware Day – historical perspectives

# Table of Contents

# Antimalware Day – historical perspectives

*David Harley, ESET Senior Research Fellow*

I'm not, some will be surprised to hear, the oldest person still active – in a sluggish sort of way – in malware research. (Let's not name those who are even older!) Though there are certainly younger people who nevertheless have been in the business longer than I have – over three decades, since you ask, though I 'only' got involved with malware in 1989.

Still, it's been a few years, and even if I wasn't in from the very beginning, I've written quite a bit about the early days, despite having caught up with some of those events by sitting (metaphorically speaking) at the feet of others. So I suppose that it's not too surprising that sometimes people contact me in the hope that my somewhat-past-their-best-by-date brains are still sufficiently intact to pick when some sort of historical perspective is required.

Recently, ESET chose to commemorate November 3rd as 'Antimalware Day, an ESET initiative to reinforce the importance of protecting against threats in a world where computers can fit into our hands.' They chose this day because November 3rd 1983 was the day on which:

*...computer scientist Dr. Fred Cohen, then a student, created a program capable of rapidly overtaking a general purpose system, as part of a university experiment. It was the first time a program like that was called a computer virus, and it meant the beginning of computer defense techniques.*

Evidently, though, it wasn't only ESET that was thinking about that anniversary. I was contacted by Spanish science journalist Javier Yanes about an article on the history of computer viruses that he was writing for the science and innovation website BBVA OpenMind, asking three related questions.

This was his first question.

*Before Cohen's program, there had been earlier codes that today are considered the first computer viruses. In your view, which one should be considered the first one, and was Cohen's program peculiar in any way that made it different from previous attempts?*

To some extent it depends on your definition of 'virus'. But in the research community, we usually consider the experimental program Creeper to be the first virus and/or worm. It was originally created at BNN Technologies by Robert H. Thomas around 1971, and ran on the Tenex operating system on Digital PDP-10s. It seems to have been more of a worm than a virus – at any rate, it's debatable whether it exactly met Cohen's informal definition:

*"A virus is a program that can 'infect' other programs by modifying them to include a, possibly evolved, version of itself."*

However, Cohen also described worms as 'a special case of viruses.'

There's actually some disagreement about what Creeper did *exactly*, but essentially it seems that it moved itself around a network by copying itself to another system and attempting to delete the previous instance. A subsequent version of Creeper by Ray Tomlinson did expand on this limited example of self-replication by allowing replication without removing the previous instance of the application. It does seem that Creeper made something of a nuisance of itself: consequently, Tomlinson also created a program called Reaper that moved around the network looking for instances of Creeper. When it found them, it would log them out, and has thus been described as the first antivirus, but it *also* spread through replication.

Apart from the fact that Cohen's first experiments were in a different operating environment ('VAX 11/750 system running Unix'), there was a difference in intent, though neither set of experiments could be described as malicious. Creeper was a demonstration of a mobile application intended for legitimate purposes: in Tomlinson's words (quoted in an article by Georgi Dalakov):

*The research effort was intended to develop mechanisms for bringing applications to other machines with intention of moving the application to the most efficient computer for its task. For example… to move the application to the machine having the data (as opposed to bringing the data to the applications) [or] to bring the application to a machine that might have spare cycles because it is located in a different time zone...*

Creeper didn't make use of a flaw in the operating system, system policy or administrative practices, and it wasn't intended to operate covertly. Cohen's experiments were not covert either: they were carried out with permission, but they were more focused on issues of computer security.

While Cohen was more receptive than most current researchers to the idea of 'benevolent' viruses such as maintenance viruses, the influence of his initial experiments and subsequent writings has been greater in terms of his ground-breaking work in defining or – at least documenting – so many of the concepts that we still rely on in the field of malware and anti-malware technology.

If you wanted to talk about viruses (or virus-like programs) as malware, you'd probably want to look at Elk Cloner, though according to Rob Slade, Elk Cloner may not even have been the first Apple II virus: he mentions reports of two 'very similar' programs coming out of discussions at Texas A&M university in 1981, whereas Skrenta reckons he wrote Elk Cloner in 9th Grade. Certainly Slade's description in his own book isn't an exact match for Elk Cloner, which he doesn't discuss at all (though some have assumed subsequently that Elk Cloner was one of the viruses he was discussing). In *Viruses Revealed* (a book Slade and I wrote together with some contributions from Urs Gattiker) we treated the A&M viruses and Elk Cloner as separate topics.

# ESET Corporate News

## ESET Launches WeLiveSecurity Website in French

ESET announced that its WeLiveSecurity website is now available in French, marking ESET's continued dedication to educating and safeguarding Canadians' businesses and their personal data.  ESET has been present in Montreal since 2009 and opened a fully-functioning Research & Development center in April 2012, which focuses on situational awareness of malware and online threats, and helps promote better public understanding of cybersecurity in general. Among other notable research, in 2014 the Montreal team received the very first Péter Szőr Award from Virus Bulletin for Best Technical Paper for its research on Operation Windigo.

ESET's prize-winning research triggered a criminal investigation from the FBI, resulting in an arrest warrant for Russian hacker Maxim Senakh. Senakh was extradited from Finland to the United States, later pleading guilty for his participation in the Windigo criminal enterprise, which saw malware being installed on tens of thousands of computer servers throughout the world, generating millions of dollars in fraudulent payments. Senakh was sentenced in August to 46 months in prison. For the first time, ESET has released the story of what happened during the four-year investigation.

Although Senakh is now behind bars, the other conspirators responsible for Operation Windigo have adapted Ebury, their flagship backdoor component, which has become stealthier than ever. ESET research has revealed that new mechanisms were added to Ebury to better hide its presence on compromised servers, effectively evading most of the Indicators of Compromise previously available. ESET has published a new set of indicators, which will give the upper hand back to server administrators fighting against attacks coming from the Windigo operators.

## Mark the First Antimalware Day with ESET

To honor the work of Dr. Fred Cohen and Prof. Len Adleman, who laid the foundations for the investigation into computer threats back in 1983, ESET declared November 3 as Antimalware Day worldwide. The objective of this day is to mark the the first use of the term "computer virus" and the subsequent and ongoing search for protection against malware of computer viruses and the constant search for protection against them.

On November 3, 1983, two computer scientists made history. Dr. Cohen, then a student, of the school of engineering at the University of Southern California, was investigating a proof-of-concept program that could have been used to infect any connected system. A prototype that Prof. Adleman later dubbed a computer virus.

This day also marks the beginning of the fight against malware, which today not only includes real computer viruses, but other types of computer threats that have triggered a never-ending search for countermeasures to protect IT systems against them.

# The Top Ten Threats

## 1. JS/Adware.AztecMedia

**Previous Ranking: 1**
**Percentage Detected: 5.23%**

JS/Adware.AztecMedia is adware - an application designed for the delivery of unsolicited advertisements. The program code of the malware is usually embedded in HTML pages.

## 2. JS/Adware.Imali

**Previous Ranking: 2**
**Percentage Detected: 3.64%**

JS/Adware.Imali is adware - an application designed for delivery of unsolicited advertisements. The program code of the malware is usually embedded in HTML pages.

## 3. JS/Chromex.Submelius

**Previous Ranking: 3**
**Percentage Detected: 2.35%**

JS/Chromex.Submelius is a Trojan that redirects the browser to a specific URL location serving malicious software. The program code of the malware is often embedded in HTML pages.

## 4. HTML/FakeAlert

**Previous Ranking: 5**
**Percentage Detected: 2.34%**

HTML/FakeAlert is a generic detection name for an HTML page showing a made-up, fake alert message, usually about a fictional virus infection or some other problem which is supposed to harm the computer or the computer user's data. The user is usually urged to contact fake technical support hotlines or to download and execute a fake security solution from the Internet to prevent "damage". This kind of page is usually used as a starting point for support scams.

## 5. SMB/Exploit.DoublePulsar

**Previous Ranking: 7**
**Percentage Detected: 2.27%**

SMB/Exploit.DoublePulsar is our name for a detection preventing the exploitation of vulnerable systems by Win32/Exploit.CVE-2017-0147.A and Win32/Filecoder.WannaCryptor malware

## 6. LNK/Agent.DV

**Previous Ranking: 6**
**Percentage Detected: 1.99%**

LNK/Agent.DV is a detection name for a *.lnk file that executes other malware and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, tricking users into believing that it's a link to drive content.

## 7. JS/ProxyChanger

**Previous Ranking: 4**
**Percentage Detected: 1.66%**

JS/ProxyChanger is a Trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses. The Trojan may redirect the victim to the attacker's web sites.

## 8. LNK/Agent.CX

**Previous Ranking: 8**
**Percentage Detected: 1.64%**

LNK/Agent.CX is a detection name for a *.lnk file that executes other malware and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, tricking users into believing that it's a link to drive content.

## 9. Win32/Bundpil

**Previous Ranking: 9**
**Percentage Detected: 1.56%**

Win32/Bundpil is a worm that spreads via removable media. The worm contains a URL from which it tries to download several files. The files are then executed and HTTP is used for communication with the command and control server (C&C).

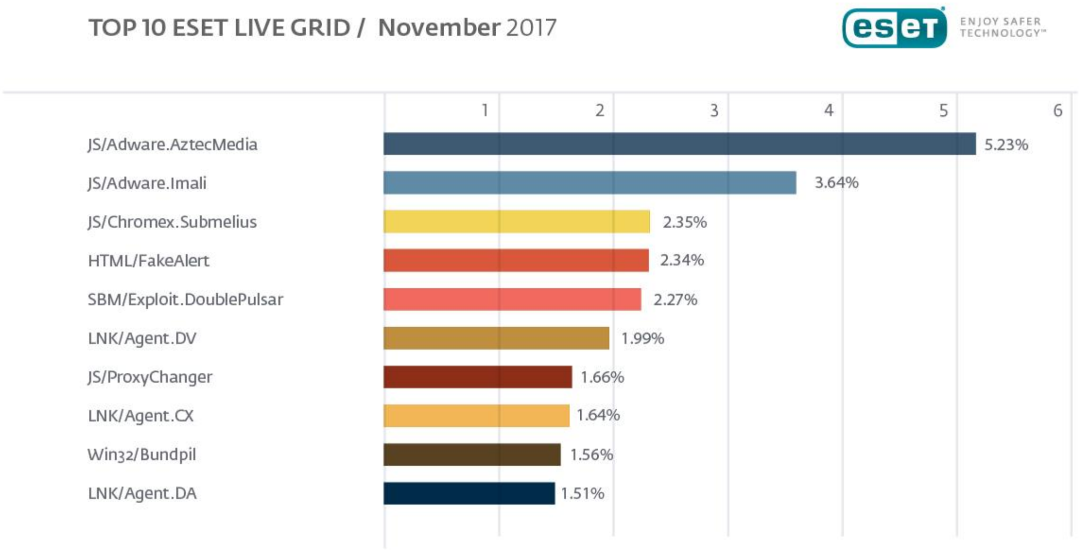
## 10. LNK/Agent.DA

**Previous Ranking: 10**
**Percentage Detected: 1.51%**

LNK/Agent.DA is a detection name for a *.LNK file that executes the Trojan Win32/Bundpil.DF. The LNK file is part of a Bundpil attack and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, convincing users that it's a link to drive content. It actually points to %system32%\rundll32.exe with a Bundpil DLL component as a parameter.

# Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the most-detected malware this month, with **5.23%** of the total, was JS/Adware.AztecMedia.



## About ESET

For 30 years, ESET® has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn 100 Virus Bulletin VB100 awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

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:

- VirusRadar
- ESET White Papers
- ESET Conference Papers
- WeLiveSecurity
- ESET Podcasts
- ESET Videos
- Case Studies