



Threat Radar

September 2015

Feature Article: Watching the Furby Fly



Table of Contents

- Watching the Furby Fly.....3
- ESET Corporate News6
- The Top Ten Threats8
- Top Ten Threats at a Glance (graph) 11
- About ESET 12
- Additional Resources 12

Watching the Furby Fly

David Harley, ESET Senior Research Fellow

This article was originally published on the [ITsecurity UK](#) web site.

Somehow, the [Furby](#), a furry toy vaguely resembling a Mogwai (the cuddly pre-Gremlin version in Joe Dante's films, rather than the demons of Chinese tradition¹) has always invited a certain amount of paranoia, fuelled by (or perhaps fuelling) the interest of the hacking community.

As well as a fairly dumb discussion on the newsgroup alt.comp.virus about its potential as a virus vector, the details of which now escape me, it was the subject of a ban of sorts on airlines. More precisely, the Federal Aviation Authority [recommended](#) that 'Furbys should not be on when the plane is below 10,000 feet', and many airlines went as far as requiring passengers 'to remove the batteries from their Furby dolls so that the electronic gizmos don't interfere with navigational systems during take-off and landing. This was as a result of the device's being classified in the same group as electronic devices such as laptops, cell phones, electronic games, and personal music devices.

'Personal stereos' at that point probably meant portable cassette and CD players rather than iPods and other mobile devices, of which modern versions certainly qualify as full-blown computers with communication capabilities that were still seen as [somewhat futuristic](#) around the turn of the century. So perhaps it's not surprising that airlines continue to extend bans and restrictions to more or less *anything* that could be described as electronic. Better safe than splattered, I suppose, however unlikely it is that any dire consequences might ensue. I certainly know people who have found that their phone or iPod had switched itself back on during a flight without any impact (so to speak) on their safe travel and arrival. No statistics seem to be available on how many successful [pocket calls](#) have been made from 30,000 feet.

In 2002 I wrote:

Furbys were recently banned in 'spy centres' because they're believed to be a possible source of information leakage. Apparently security chiefs believed that they learned phrases spoken around them and that they might therefore repeat secret information, making them a security risk. My daughter and I have spent many happy hours trying to persuade her furby to say "My hovercraft is full of eels", preferably

¹ The mythological basis of [the Dante films](#) is quite interesting in itself: the cuddly Mogwai share a name with demons that have a great deal in common behaviourally with the vengeful spirits of [Chinese tradition](#). Even their methods of reproduction and mutation bear some resemblance. The name [Gremlin](#) seems to have originated in RAF slang of the 1920s (or possibly earlier), used to describe creatures deemed responsible for 'inexplicable' mechanical failures, the term passing into wider currency through [a book by Roald Dahl](#).



in a Ukrainian accent, but have so far failed miserably. Neither the accompanying instruction manual nor www.furby.com seem to be aware of this splendid ability, but perhaps it's undocumented, like the opcode which is supposed to enable a malicious hacker to burn out a Pentium motherboard.

This particular ban [seems](#) to have been based on the widely-held belief that Furby's learn to speak English rather than their 'native' Furbish (yes, I know...) in much the same way that humans are assumed to learn, [by repeating what is said to them](#). Which may or may not be what Tiger Electronics initially wanted its young customers to believe: in any case, the product description for the Furby Boom still tells them to 'Talk to your Furby and interact with it to teach it English and shape its personality'.

However, when the story broke, its executives went out of their way to point out that Furbys had no recording mechanism. As for the learning process, it appears that the 'learning mechanism' and repetition of speech was based on reinforcement of uttering *pre-programmed phrases*, not learning through [mimicry](#). Apparently, petting the toy when it spoke encouraged it to repeat the phrase more often, but the only thing it was learning was the listening preferences of its owner. It is apparently designed to introduce more pre-programmed English phrases over time in order to reinforce the false impression that it is actually *learning* English. In any case, it [appears](#) that the NSA rescinded its ban. I'm not sure if it carried out any investigation into the reading ability and gullibility levels of its own executives, or into whether NSA-employed Furby owners were offered alternative stress alleviation strategies.

So what about the 'hacking' aspect? Mostly, this is concerned with hacking in its old-fashioned, non-pejorative/non-malicious sense, in particular with manipulating the toy's audio and sensory inputs for circuit bending, specifically (in this case) to generate audio effects. However, an article from December 2013 by Michael Coppola - [Reverse Engineering a Furby](#) – demonstrates a wider interest, specifically in the inter-device protocol used by recent models, and pointed to [earlier research](#) on the events it understands.

In spite of Coppola's invocation of the dreaded [#badBIOS](#), inspired by [the use](#) of an audio protocol that encodes data into bursts of high-pitch frequencies for communication between the Furby and an iOS mobile app (or with other Furbys) that brings to mind Dragos Ruiu's [claims](#) – [not universally accepted](#) – of the existence of malware that (among other things) communicates between infected devices using [ultrahigh speaker frequencies](#), I'm not seeing a malware-friendly supertool here, though the articles concerned are actually fascinating, in a nerdish sort of way. However, that didn't stop Coppola's research being cited as having discovered 'vulnerabilities in the way the toy communicates with other Furby toys and its mobile app' in an article sensationally entitled [Valasek: Today's Furby Bug is Tomorrow's SCADA Vulnerability](#).

I wasn't at the [Security of Things event](#) where Valasek talked about Coppola's work, of course, but what he actually said turns out to be a little less sensational.

'...low-impact research cannot be dismissed either. Not every IOT vulnerability is going to be high impact. You have to judge how technology that might be vulnerable today will be used in the future.'



Nor was I at the [events in 2014](#) where Coppola apparently talked about a 'delicious 0-day', but I presume that it was interesting but, as Valasek puts it, low impact. A lot of effort involving various highly corrosive acids and an electronic microscope doesn't seem to have uncovered all of Furby's furry little secrets. Moving from what may be known to the next big thing in SCADA hype may be premature, even if it does result in another Establishment [panic attack](#) at some point.

My daughter moved on from Furby and [Tamagotchi](#) quite a few years ago, but if I found one of my grandchildren with one, I don't think I'd be ripping it out of his or her hands and looking for the nearest junkyard with a car crusher just yet. And while I'm not about to underplay [the risks to national infrastructure](#), it's all too easy for speculation to [spill over into fantasy](#).



ESET Corporate News

[ESET Acquires Data Encryption Leader DESlock+](#)

[ESET](#)® announced the acquisition of data encryption company DESlock+. ESET plans to fully integrate the DESlock+ core technology into its existing business and consumer product lines. Data protection and privacy are among the top concerns of both companies and individuals, with government agencies enforcing regulations that require businesses and organizations to implement security measures, including encryption, to protect the data of their users.

“A recent survey we conducted among businesses shows that two out of every three companies see a need for encryption as part of their standard endpoint security solutions,” said Ignacio Sbampato, Chief Sales and Marketing Officer at ESET. “We had very good results offering DESlock+ encryption solutions as part of our ESET Technology Alliance, and we believe our customers will be very happy to see that we are taking that partnership even further. Acquiring DESlock+ will allow us to complement our ESET Security products with a great encryption technology.”

DESlock+, based in Taunton, England, specializes in advanced encryption solutions and has been a successful partner within ESET’s Technology Alliance since 2013. With the acquisition, ESET has also added a new Research & Development location, which will increase the company’s ability to recruit local talent in the UK.


[ESET Releases Next Generation of ESET® Mail Security for Microsoft Exchange Server](#)

[ESET](#)® announced the release of a new generation of [ESET Mail Security for Microsoft Exchange Server](#)® with a completely redesigned user interface, enhanced anti-spam engine, and antivirus with optional cloud-powered scanning. Supported by [ESET Remote Administrator 6](#)®, the product provides a secure email experience with malware protection, spam filtering and thorough e-mail scanning.

The new features of ESET Mail Security for Microsoft Exchange Server simplify administration and deliver improved security functionality for IT administrators. To make it easier for company administrators to manage company mail flow more efficiently, ESET introduced Local Quarantine Management. This tool blocks what it finds to be malicious, but gives the mail recipient an option to access messages as needed. If a legitimate message is blocked, individuals can retrieve the email quickly, allowing workflow to continue uninterrupted.

Additionally, Local On-Demand Scan decreases the need to overstress server resources by allowing admins to choose which specific databases and mailboxes to scan. The solution also allows easy access to relevant logs of server activity, so that troubleshooting is one click away.

The new layers of protection featured in ESET Mail Security 6 for Microsoft Exchange Server shield both the host server and the endpoints



from receiving mail from evolving threats. Additional features include:

- **Advanced Memory Scanner** – Strengthens protection against heavily obfuscated and/or encrypted malware
- **Exploit Blocker** – enhances protection of frequently-exploited applications, such as web browsers, PDF readers, email clients or MS Office components
- **Anti-Phishing** – Scans the content of e-mail messages for links or scripts that might mislead users or trick them into visiting malicious websites

Find more information about the next generation of ESET Mail Security 6 for Microsoft Exchange at

<http://www.eset.com/us/products/email-security-microsoft-exchange/>



The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 6.08%

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 command and control server (C&C) to receive new commands. The worm may delete files with the following file extensions:

- *.exe
- *.vbs
- *.pif
- *.cmd
- *Backup

2. JS/TrojanDownloader.Iframe

Previous Ranking: N/A
Percentage Detected: 1.84%

JS/TrojanDownloader.Iframe is a trojan that redirects the browser to a specific URL location serving malicious software. The malicious code is usually embedded in HTML pages.

3. Win32/Adware.Mobogenie

Previous Ranking: N/A
Percentage Detected: 1.81%

Win32/Adware.Mobogenie is a Possible Unwanted Application associated with Mobogenie, a PC program to manage Android devices. Once installed on the system, usually without the user's knowledge, it is intended to download and/or display unsolicited advertisements.

4. HTML/ScrInject

Previous Ranking: N/A
Percentage Detected: 1.73%

Generic detection of HTML web pages containing obfuscated scripts or iframe tags that automatically redirect to the malware download.



5. LNK/Agent.AV

Previous Ranking: 4
Percentage Detected: 1.66%

LNK/Agent.AV 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.

6. LNK/Agent.BX

Previous Ranking: N/A
Percentage Detected: 1.52%

LNK/Agent.BX 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.

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/TrojanDownloader.Waski


Previous Ranking: N/A
Percentage Detected: 1.33%

Win32/TrojanDownloader.Waski is a Trojan that uses HTTP to try to download other malware. It contains two URLs and tries to download a file from the addresses. The file is stored in the location %temp%\-miy.exe, and is then executed.

9. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.32%

This is a file infector that executes every time the system starts. It infects .dll (direct link library) and .exe executable files and searches for htm and html files into which it can insert malicious instructions. 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.

10. INF/Autorun

Previous Ranking: 9

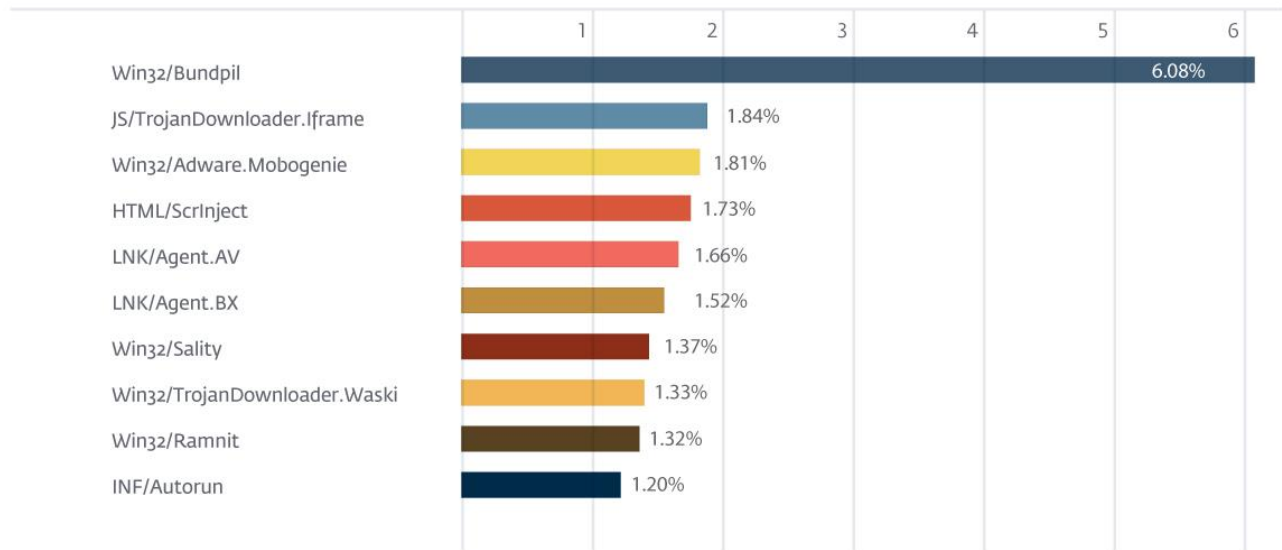
Percentage Detected: 1.20%

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 malicious executable. This file is usually dropped into the root folder of all the available drives in an attempt to auto-execute a malicious executable when the infected drive is mounted. The malicious AUTORUN.INF file(s) may have the System (S) and Hidden (H) attributes set in an attempt to hide the file from Windows Explorer.

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 6.08% of the total, was scored by the Win32/Bundpil class of treat.

TOP 10 ESET LIVE GRID / September 2015





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 has continued to lead the industry in proactive threat detection. By obtaining its 91st VB100 award in April 2015, 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 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](#)