May 2015
Feature Article: Nepal earthquake scam: out for a duck…

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Nepal earthquake scam: out for a duck…

(But there are plenty more where he came from…)

David Harley, ESET Senior Research Fellow

[A slightly shorter version of his article was originally published on the AVIEN blog. The AVIEN tech-support scam resource page was also updated to include this article from WeLiveSecurity: Tech Support Scammers with Teeth].

It was, I suppose, inevitable that the earthquakes in Nepal would provide an opportunity for scammers to capitalize on the misery of others. I hadn't been tracking this particular subcategory of scamming nastiness, but a pingback on one of my articles written in 2011 for the AVIEN blog about Japanese earthquake-related scams and hoaxes – actually, a link to some of the many articles relating to those scams – drew my attention to a blog article by Christopher Boyd for Malwarebytes on Nepal-related scams.

In that article, he highlights a bizarrely-expressed donations scam message claiming to be from the weirdly named 'Coalition of Help the Displaced People':

We write to solicits [sic] your support for the up keep [sic] of the displaced people in the recent earth quack [sic] in our Country Nepal.

He also flags an assortment of Nepal themed scam emails listed at Appriver, and a 'dubious looking donation website' covered in detail by Dynamoo.

Appriver's collection includes:

- A classic 419 claimed to be from one of the earthquake victims (daughter of a deceased politician – stop me if you've heard this story before…)
- Another giving the impression it's on behalf of the Salvation Army and World Vision: who'd have guessed that big organizations like those would use Gmail accounts? ;)
- An exercise in guilt tripping from 'Himalaya Assistance' whose real purpose seemed to be to distribute a keylogger.

US-CERT also warns of 'potential email scams'. As well as generic advice about mistrusting links and attachments and keeping security software up to date, the alert very sensibly advises the use of the Federal Trade Commission's Charity Checklist. The FTC's page includes sections on:

- Signs of a Charity Scam (including some heuristics that work with all sorts of types of contact, not just email)
- Charity Checklist (how to ensure your money is going where you intend it to go)
- Charities and the Do Not Call Registry
- Report Charity Scams

There are a number of ways of checking the bona fides of a charity, including Charity Navigator (http://www.charitynavigator.org/) and Charity Watch, formerly the American Institute of Philanthropy (http://www.charitywatch.org).

In the UK, GetSafeOnline also has a guide to protecting yourself from charity scams, including resources for checking the status of UK charities:

- Charity Commission for England and Wales
- Office of the Scottish Charity Regulator
- Charity Commission for Northern Ireland
- The Fundraising Standards Board (FRSB)

The FBI advise that suspected Nepal-earthquake-related fraud should be reported to the toll-free 24/7 National Center for Disaster Fraud hotline at 866-720-5721, and that disaster fraud victims can contact the Center on that phone number, by fax at 225-334-4707, or by e-mail at disaster@leo.gov.

At a bit of a tangent from the 'watch out for scams' message, I can't help noticing that quite a few of the articles that offer advice on verifying that charities are genuine also make a point about evaluating what amounts to the quality and efficiency of the charity according to the percentage of its funds that is actually donated. Huffington Post, for example, suggests:

Not only do you want to make sure that the charity you're donating to actually sends funds to the disaster victims you want to help, but it's also wise to find out what percentage of donations made actually go to relief -- some charities, while legitimate, only donate very little of their profits to people and causes in need.

Fair enough as regards charities that provide disaster relief, perhaps, but simplistic. Very few charities are wholly about direct relief of a disadvantaged group. For instance, last autumn there was a lot of fuss in the wake of the 'Ice Bucket Challenge' craze about the fact that only 27% of the funds raised for the Amyothrophic Lateral Sclerosis Foundation were expected to be spent on research: however, the attacks picked up the social media muttering about 'huge' salaries (actually much lower than you'd expect to see in the private sector) and administrative overheads disregarded the fact that ALS has a three-pronged programme including not only medical research, but also patient and community services (19%) and public and professional education (32%). I'm certainly not going to say that no money is wasted in the charity sector (*or* the state sector, *or* the private sector) but if you're going to talk about waste, you really need to understand what the aims of an organization actually are, and that budgeting is an ongoing process depending on many variables, not a simple static calculation.

As for those who cynically exploit the misfortunes of others purely for the benefit of their own wealth, I'll leave the last word to Chris Boyd, since I couldn't agree more and couldn't have put it any better:

Scammers riding on the coat-tails of disasters are the lowest of the low, and we need to remain vigilant in the face of their antics – every time they clean out a bank account, they're denying possible aid to the victims of the quake and *creating all new misery elsewhere. That's quite the achievement…*

How did the Internet change the everyday work of a security researcher?

Sabrina Pagnotta, ESET Corporate Communications Analyst

[This article was previously published on WeLiveSecurity just before World Telecommunication and Information Society Day 2015].

Every May 17th is **World Telecommunication and Information Society Day**, which attempts to raise global awareness on how the Internet and new technologies changed our society, and the opportunities they gave to improve our lifestyle. This special date, also known as Internet Day in some Spanish-speaking countries, is an opportunity for us at ESET to celebrate its existence by remembering what it was like to work in security **before the Internet** appeared.

What do you think it was like to do the everyday work of a security researcher in the 1980's? What has changed in terms of protection against threats? And, how has the procedure to find and investigate security issues changed?

This and other queries were answered by two of ESET's respected security researchers, with decades of experience and a lot of stories to tell: **Aryeh Goretsky** and **David Harley**.

ESET's Distinguished Researcher Aryeh Goretsky has been around technology and computers ever since he used a ***Commodore PET*** *for the first time in the late 1970's. Having worked now for some two-and-a-half decades in this industry, he has an interesting point of view when it comes to the rise of the Internet:*

I suppose the Internet has been something of a mixed blessing for me. While it has enabled all sorts of means of communication that simply were not possible before (think instant messaging) as well as allowing existing lines of communication to occur at faster rates, it has also allowed **malicious code** to spread orders of magnitude **more quickly** than it previously could: before that, network connections often meant computers calling each other with modems over telephone lines, or overnighting a set of floppy diskettes or CDs by courier, since that was faster than the network communications we had.

In the beginning, we used to say that **computer viruses spread** at the speed at which courier and postal services could ship and deliver infected floppies. Nowadays, a worm or other malware can become **globally pandemic** in an hour or two.

Meanwhile, ESET Senior Research Fellow David Harley started his career in information technology in the 1980's and, ever since, he says industry puts up with him because, well, he's been around so long –having written a number of Internet FAQs and articles on programming and security back when those were issues that most people didn't think of as being important to them.

In the 1980s, when I moved into information technology as a career, the Internet had already existed for a couple of decades – in fact, some of its underlying technologies, notably the telephone system, are far older. Nonetheless, it was a very different environment. There was no **World Wide Web** as such, though there were protocols and utilities subsequently assimilated into and/or replaced by web browser technology (*archie, gopher, and veronica*).

Access to the handful of machines that were permanently connected to the Internet was usually filtered for home users through services like AOL. Until I left the UK's National Health Service in 1989, my **online communications** with the outside world were mostly restricted to services that sidestepped the 'proper' Internet – bulletin boards and the UK's Prestel videotex/Viewdata system (rather like the teletext systems that have been gradually vanishing from television in recent years).

Moving to the Imperial Cancer Research Fund (now merged into Cancer Research UK) gave me direct access to more **hardware** – one of the (then) new 80386-driven PCs, a Mac IIcx, and a Sun workstation – but even when we got our own **permanent connection to the Internet**, it was limited to terminal access to a server in the NOC (Network Ops Centre) via *telnet*, *kermit*, and *FTP*. Still, it gave me access to **useful resources** such as mailing lists, security newsgroups, and vendor web sites.

And when I first began to **work from home** – using a US Robotics modem borrowed from work that cost more than my own PC and occupied almost as much space as a trio of 12" baguettes – I was able to add those resources to my home access to CIX and Compuserve (which both already gave me email, and access to various useful forums). Indeed, it's through all these resources that I first met (virtually at any rate) many of the people I work with now (inside and outside ESET), and work I did on **Internet FAQs** provided a basis for some of my early articles, papers and books.

So how did the Internet change our lives and what new possibilities emerged? Aryeh Goretsky says:

The Internet changed not just how people did existing things on their computers, like writing letters or drawing pictures, but gave rise to **new services** as well. Electronic banking existed well before—it was available on some dial-up services like CompuServe, Prodigy and QuantumLink, to name a few—but it was not until ISPs came onto the scene that **banking** followed, eager to give their customers new conveniences and services.

PayPal emerged as the de-facto standard for person-to-person **financial transactions**, and even criminals had their own payment systems, like e-gold and Liberty Reserve. With all of this **money moving around the web**, it wasn't long before criminals looked for ways to steal it, and today, most financial crimes use computers instead of guns to accomplish their thefts.

While according to David Harley:

By 2001, **Windows** and **Mac** machines were able to make good use of the Internet and the Web in and out of the office. Indeed, working from home (which I've done full-time since 2006) tends to give the computer user **more control** and wider scope in terms of the **services and applications** used, at any rate if s/he uses his or her own device and is not reliant on an employer for Internet access.

The flipside is that users were more able to **put themselves in harm's way** when the IT unit wasn't responsible for their connection: by that time there was a lot more to worry about than infected floppy disks, with **threats of all sorts** capable of traversing the ether almost **instantaneously**, and keeping up with security news and having good network protection was more important than ever. Of course that hasn't changed with the onset of BYOD/CYOD.

And what does this mean for a security researcher? Aryeh Goretsky says there's a challenge:

It means that things move much faster, and as a result, we have to **respond more quickly**. Fortunately, the same Internet which empowers all the positive things allows us to communicate more efficiently as well, sharing threat intelligence and data.

And that means we can do things like **leverage the power** of the advances in networking, software and hardware that allow the Internet to run at scale not just to **distribute** things like updates more quickly than before, but reduce false positives, compatibility issues and other types of problems that plagued the old reactive kinds of anti-virus software that were reactive.

That being said, David Harley concludes:

The Internet gives me access to my colleagues at ESET, specialist mailing lists that share threat intelligence (and much else), the media, and a multitude of resources that simply didn't exist or were impossible to find in the early 90s. Of course it's **easier to publish** timely commentary (or papers, manuals, FAQs and so forth) with standard blogging and CMS tools than it was with *lynx* on a Unix server, and **researching the topics** for that content is far easier.

However, those advantages also have a flipside. The interactive nature of today's web means that there is **more information (and misinformation)** out there than any one person can ever hope to gather and verify, unless it concerns an unusually esoteric topic.

It's easier for someone who already has expertise in a particular field to **select and evaluate** information from that field, of course, but what is the everyday user supposed to do when anyone with a laptop – or even a cell phone – can find somewhere to say what they like?

ESET Corporate News

Cybersecurity Leader ESET Reaches Record-High Employment Numbers

ESET® announced recently that the company has grown more than 90 percent in the last 10 years, with 1,000 employees now working across the globe. ESET North America has also reached a record number of employees at its San Diego, Calif. headquarters, and accounts for more than 20 percent of ESET personnel worldwide.

Further growth is expected in North America this year, with job openings at the San Diego headquarters and the malware research lab in Montreal. Additional Northeastern expansion is expected later this year. Recent notable hires in the San Diego office include Vice President of Sales, Gerald Choung, and Director of Channel Marketing, Hope McCluskey.

In support of the company's global hiring efforts, ESET has launched several new recruiting games, available at JoinESET.com. The online games are aimed at attracting new programming and coding talent to the company by offering interactive challenges. The same programming strategies employed in the games are utilized by ESET researchers and analysts on a daily basis to ensure the superior reliability of its products.

ESET Unveils Small Business Cybersecurity Survival Guide for National Small Business Week

ESET® has released a Small Business Cybersecurity Survival Guide in support of National Small Business Week, celebrated this week. This unique resource outlines the biggest risks small businesses face and how they can best defend themselves from the latest cyber threats.

Verizon* found that 62 percent of cyberattacks occurred in smaller organizations. Additionally, IDC predicts* security spending by small businesses this year is expected to be 10 to 12 percent higher than in 2014. In response to the growing demand and necessity for cybersecurity policies, ESET created their Small Business Cybersecurity Survival Guide to share strategic advice from security experts on what precautions small businesses should take to protect themselves and their customers' private data from falling into the wrong hands.

While cybersecurity may seem intimidating to some, the guidance that ESET outlines in the new guide is as easy as knowing your "ABCs" and includes:

- Assess your assets, risks, resources – Understand all possible targets and threats.
- Build your policy – Spell out protective measures and ensure leadership prioritizes security.
- Choose your controls – Decide what appropriate tools are needed to enforce a security policy.
- Deploy controls – Ensure protection methods are in effect and are appropriate for the business.
- Educate employees, execs, vendors – Spread awareness and gain the buy-in of the full team.
- Further assess, audit, test – Ensure regular evaluation and additions to policy in place.

The Top Ten Threats

1. Win32/Adware.MultiPlug

Previous Ranking: 1
Percentage Detected: 3.39%

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.

2. Win32/Bundpil

Previous Ranking: 2
Percentage Detected: 2.03%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address 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 folders:

*.exe

*.vbs

*.pif

*.cmd

*Backup.

3. JS/Kryptik.I

Previous Ranking: 3
Percentage Detected: 1.97%

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.

4. LNK/Agent.AV

Previous Ranking: 5
Percentage Detected: 1.45%

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.

5. Win32/AdWare.ConvertAd

Previous Ranking: 9
Percentage Detected: 1.36%

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

6. Win32/Sality

Previous Ranking: 6
Percentage Detected: 1.33%

Sality is a polymorphic file infector. When 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

7. 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.

8. INF/Autorun

Previous Ranking: N/A
Percentage Detected: 1.18%

INF/Autorun is a generic detection of 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.

9. Win32/Packed.VMProtect.AAA

Previous Ranking: N/A
Percentage Detected: 1.17%

Win32/Packed.VMProtect.AAA is a generic detection of malware protected with AntiVM code.

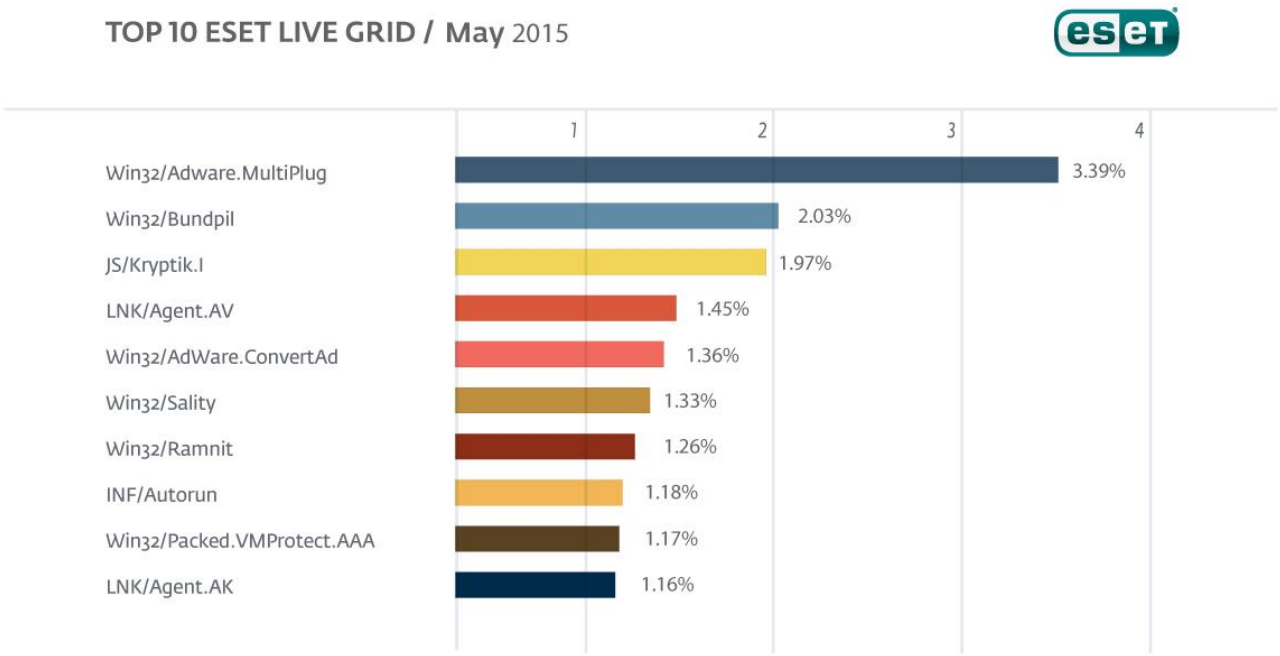
10. LNK/Agent.AK

Previous Ranking: N/A
Percentage Detected: 1.16%

LNK/Agent.AK 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. This vulnerability became known at the time of discovery of Stuxnet, as it was one of four vulnerabilities that were executed by Stuxnet variants.

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 3.39% of the total, was scored by the Win32/Adware.MultiPlug 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