November 2016
Feature Article: Careers Fighting Cybercrime

ESET ENJOY SAFER TECHNOLOGY™

Table of Contents

Careers Fighting Cybercrime

David Harley, ESET Senior Research Fellow

This article originally appeared on WeLiveSecurity

One of the ways in which STOP. THINK. CONNECT.™ - which describes itself as 'the global online safety awareness campaign to help all digital citizens stay safer and more secure online' works towards achieving its aims is by inviting participating partners such as ESET to offer tips and advice in the course of its frequent Twitter chats (#ChatSTC).

On October 20th, the subject of one of these events was Recognizing and Combating Cybercrime (the link leads to the entire chat). These generally take the form of commentary from a wide range of organizations in response to specific questions. A particularly interesting question – well, it interested me – was Question 11.

Q11: What are some examples of cybercrime-fighting careers, and what skills are needed for a cybersecurity job?

Not that I have a secret yearning to launch a new career in careers counselling, but I do actually get asked to give such advice quite a lot, probably because people think someone as old as I am, after 30 years or so in or on the borders of the security business, must have something useful to say. That may be optimistic on their part, given my somewhat random career path, but I'll come back to that below. In the meantime, here are some articles cited by @ESET in that Twitter chat that address the topic.

- "The future health of our security requires a more diverse workforce. Here are some resources that can help." [A pointer to an excellent article by Lysa Myers on addressing the all-too-obvious gender gap in IT security, with lots of useful links. – DH]

- "For parents of kids who'd like to get into security, these tips will help nurture their genius." [Fortunately, you don't have to be a genius to get a job in IT security, else I'd probably be working in a bar. Come to think of it, that's not a bad idea. Anyway, some useful thoughts in this more generic article.]

- "If you're looking to start a career in cybersecurity, this post has some great tips and links." [Another article by Lysa Myers, again with useful links.]

- One of our researchers, @dharleyateset gives some insights on "what it takes" here."

That last entry requires a little explanation, since it's not an ESET link. Earlier in 2016, Matt Ashare contacted me on behalf of OnlineEducation.com, asking several interesting questions relating to working in IT security, to which I responded at some length over the next few weeks. (I hasten to add that I was by no means the only person he interviewed in this way: among others were my friend – and sometime co-author – Robert Slade, and Kelly Jackson Higgins, Executive Editor at Dark Reading.)

The questions we were asked were as follows:

- Can you provide a rough outline of what cybersecurity has come to mean as a discipline and a career? How has it come to be incorporated into the larger fields of IT and computer science/programming?
- With that in mind, what should we be teaching the next generation of IT and computer science specialists about cybersecurity?
- On a practical level, what does the day-to-day work of cybersecurity look like, and what kind of person/personality is well suited to this kind of work?
- What kinds of coursework and practical training should students look for in an advanced degree in cybersecurity, and what kind of experience outside of the classroom are helpful in cultivating expertise in the field?
- How did you get into the field, what drew you to it, and how have you seen it evolve over the last decade or so?
- What are employers looking for in cybersecurity hires and how should someone who's aiming to enter the field prepare him or herself?
- What should we be teaching the next generation, and even the current generation of information security specialists and technicians, both in terms of skills and ethics?
- How is the interplay between government policies, technological innovations, economic forces, and social dynamics impacting the evolution of cybersecurity, and what are the biggest factors shaping education and employment in the field?
- From your perspective, what are the one or two biggest misconceptions that people seem to have — even people "in the know" — about cyber attacks, malware, and information security?

Those seem to me to be questions that may well interest people contemplating a career path in security, and if nothing else you'll get a wide range of viewpoints. And if all that seems a little daunting, you could try the comprehensive summary elsewhere on that site that includes quotes from several of us, plus a lengthy list of further resources: Guide to Careers in Cybersecurity, Information Assurance and Digital Forensics.

ESET Corporate News

ESET Endpoint Security Receives Top Performance Score According to AV-Comparatives

AV-Comparatives has published a special Network Performance Test, wherein 6 major business security suites were tested. The Network Performance Test compared resource utilization and management by six endpoint security solutions, testing their impact on valuable business resources such as network traffic and machine load (CPU and RAM). Updates that are large in size have direct ramifications for company networks, reducing valuable bandwidth that could be used for other business critical functions.

ESET achieved the highest ratings in an additional test determining the file size of client-side definitions. Compared to Symantec, whose virus definition file size is 700 MB, ESET's is 10 times smaller. This result is another confirmation of ESET's key benefit to IT and network administrators – its small footprint in terms of network traffic. Large virus definition file sizes can drain a company's network and lead to latency issues. ESET Endpoint Security runs smoothly, having minimal impact on business environments.

For more information about ESET's performance in AV Comparatives' tests, please visit: https://www.eset.com/int/business/av-comparatives-network-performance-test/ .

ESET offers free tools against dangerous banking malware and Crysis ransomware

ESET released a free decryptor for ransomware victims, offering a helping hand to anyone whose data or devices have been hit by the Crysis family Win32/Filecoder.Crysis. The tool was prepared using the master decryption keys, recently released via a forum on BleepingComputer.com.

In addition, due to the recent increase in infections by the Retefe Trojan, ESET launched a Retefe Checker website, where users can download a free tool that automatically checks the computer for indicators of the presence of the Trojan. Uncovered by ESET's research team, the Retefe Trojan is capable of redirecting its victims to modified banking pages to harvest login credentials. This is why ESET researchers have noticed that the users of certain bank services are anxious to check if their computers are infected.

For a more detailed report on the recent findings, visit https://www.eset.com/us/resources/detail/eset-releases-free-crysis-ransomware-decrytor-tool/ and http://www.welivesecurity.com/2016/11/10/tesco-bank-not-alone-targeted-retefe-malware/

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 14.36%

JS/Danger.ScriptAttachment is a generic detection of suspicious e-mail attachments.

2. Win32/TrojanDownloader.Wauchos

Previous Ranking: 2
Percentage Detected: 6.26%

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, including settings and the computer's IP address. Then, it attempts to send the information it has gathered to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

3. LNK/Agent.DA

Previous Ranking: 4
Percentage Detected: 3.34%

LNK/Agent.DA is 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.

4. Win32/Bundpil

Previous Ranking: 5
Percentage Detected: 3.2%

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) to receive new commands. The worm may delete files with the following file extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

5. Win64/TrojanDownloader.Wauchos

Previous Ranking: 6
Percentage Detected: 3.01%

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer's IP address. Then, it attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

6. JS/ProxyChanger

Previous Ranking: 9
Percentage Detected: 2.58%

JS/ProxyChanger is a Trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses.

7. JS/TrojanDownloader.FakejQuery

Previous Ranking: N/A
Percentage Detected: 2.52%

JS/TrojanDownloader.FakejQuery is usually located on a legitimate HTML page and its main purpose is to load malicious content (from a malicious source) into this page.

8. HTML/Refresh

Previous Ranking: 9
Percentage Detected: 1.75 %

HTML/Refresh is a Trojan that redirects the browser to a specific URL serving malicious software. The malicious program code is usually embedded in HTML pages.

9. HTML/FakeAlert

Previous Ranking: 8
Percentage Detected: 1.52%

HTML/FakeAlert is 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 user's data. The user is usually urged to contact fake technical support hotlines or 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’.

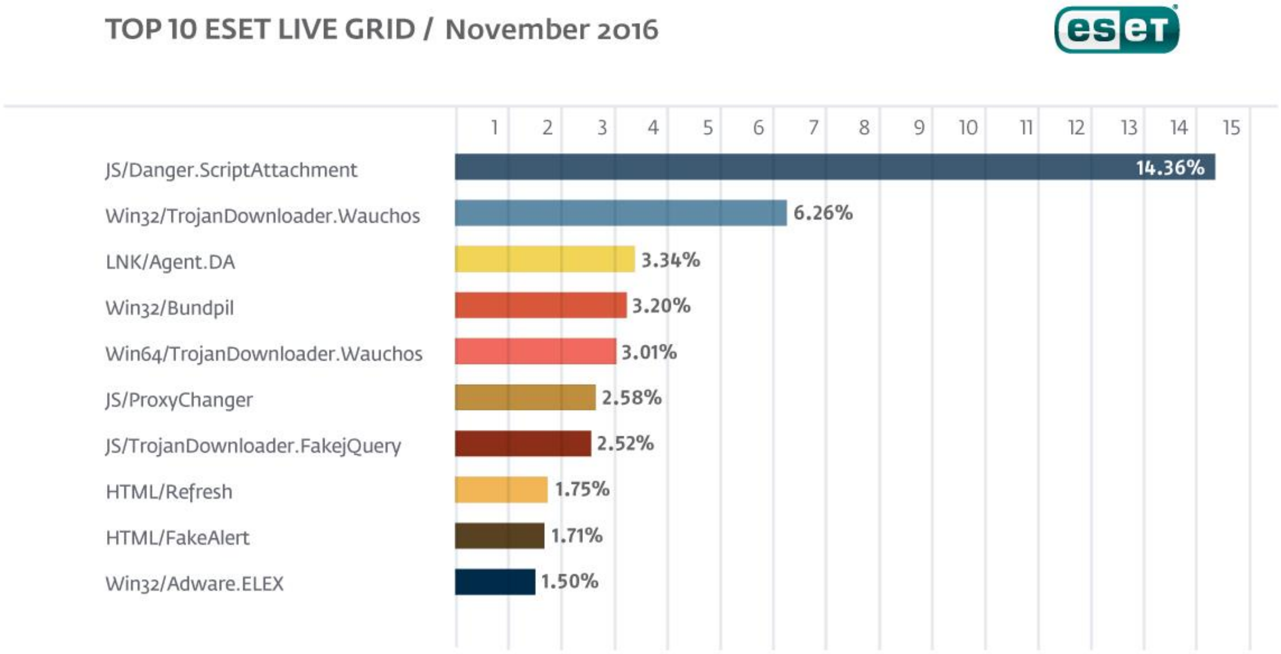
10. Win32/Adware.ELEX

Previous Ranking: N/A
Percentage Detected: 1.5%

Win32/Adware.ELEX is an application designed for delivery of unsolicited advertisements to an affected computer. Usually, it alters the behavior (settings) of an Internet browser (for example adware sets its own “homepage” and setting back this value to original value is no easy task - the adware or a component of the adware is protecting this setting). Then the adware displays small windows with advertisements within the browser.

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 14.36% of the total, was scored by JS/Danger.ScriptAttachment.



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 the 97th award in July 2016, 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 the United Kingdom, 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:

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

ENJOY SAFER TECHNOLOGY™