Interview Question

Convert a string to an integer without built-in functions.

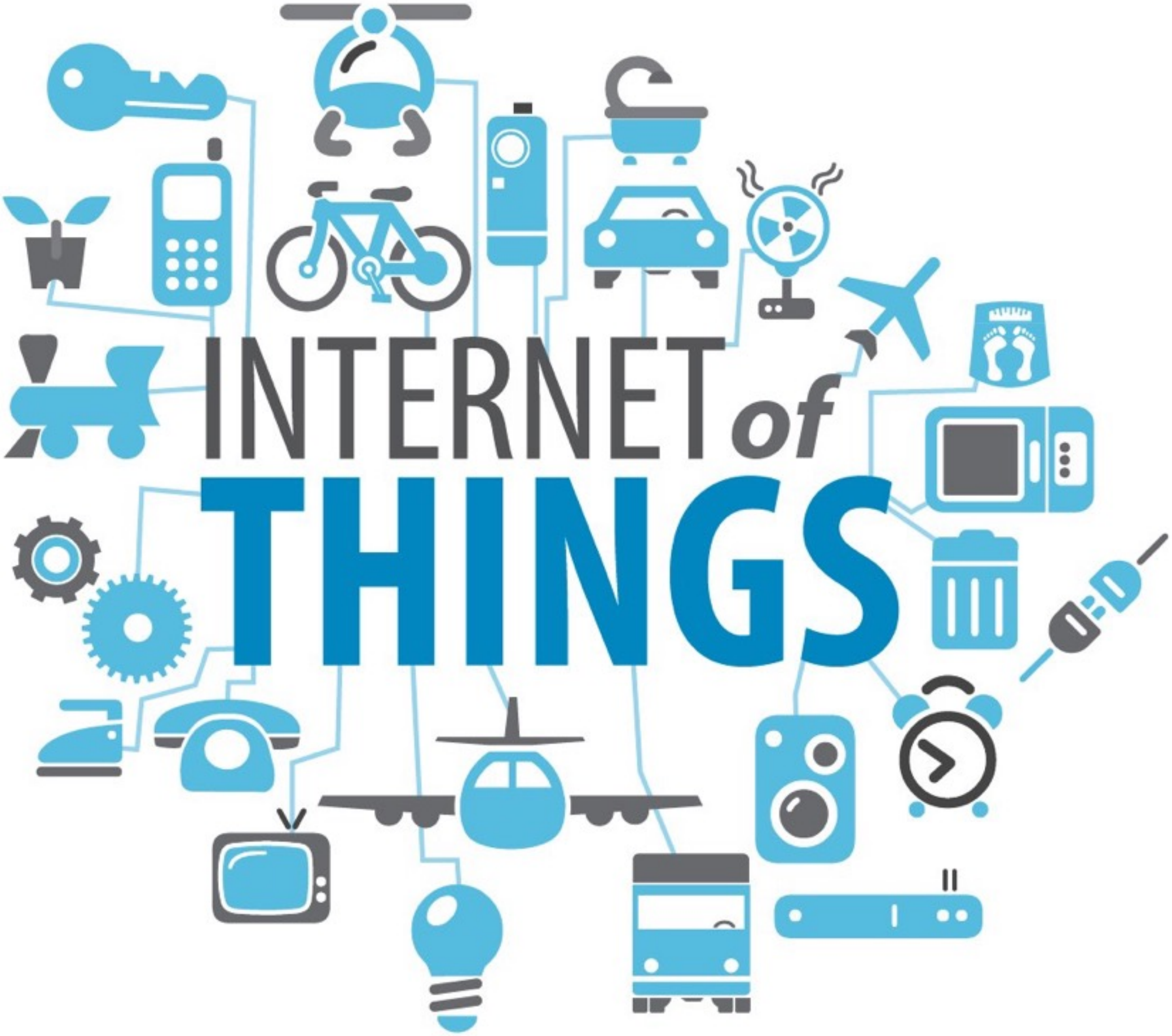
Homework Question

(Actual Google Interview Question)

Given a string, find the longest palindrome within the string in linear time (a palindrome can span multiple words, or be parts of words)

Solution

```
 8      public static int stoi(String s)    {
 9          int rv = 0;
10          boolean neg = false;
11          if (s.charAt(0) == '-')    {
12              neg = true;
13          }
14          for (char c : s.toCharArray())    {
15              if (c == '-')
16                  continue;
17              rv *= 10;
18              rv += c - '0';
19          }
20          if (neg) rv *= -1;
21          return rv;
22      }
```


INTERNET of
THINGS


NORSE
ATTACK ORIGINS
COUNTRY
ATTACK TARGETS
COUNTRY
Cyberspace Warfare
The Future of National Conflict
LIVE ATTACKS
TIMESTAMP
ATTACKER
ORGANIZATION
LOCATION
IP
TARGET
LOCATION
TYPE
SERVICE
PORT
ATTACK TYPES
SERVICE
PORT

Who Are the Players?

People’s Liberation Army

3PLA

Who Are the Players?

People's Liberation Army

3PLA

Who Are the Players?

People's Liberation Army

3PLA

Chen Ping

Codename: cpyy

Unit 61486

Suspected of numerous attacks against US aerospace industry

Believed to be responsible for domain acquisition

Who Are the Players?

People's Liberation Army

Chen Ping

Codename: cpyy

Unit 61486

3PLA

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

Charged with 31 counts of felony hacking against six US steel companies based in PA

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

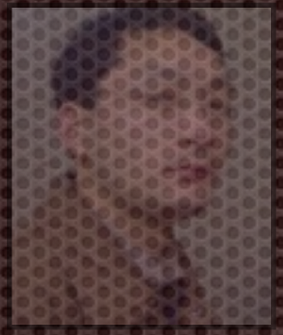
Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Gu Chunhui



Wen Xinyu

S

Wang Dong

Huang Zhenyu

United States Military

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

United States Military

UNITED STATES CYBER COMMAND

Who Are the Players?

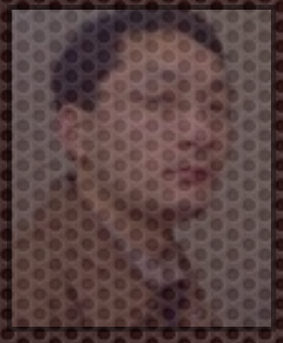
People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit

Gu Chunhui



Wen Xinyu

Sun Ka

Wang Dong

Huang Zhenyu

United States Military

24

TWENTY-FOURTH AIR FORCE

UNITED STATES CYBER COMMAND

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

United States Military

UNITED STATES CYBER COMMAND

24

TWENTY-FOURTH AIR FORCE

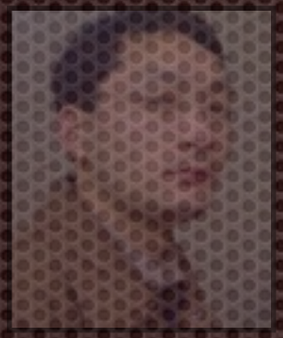
Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3P

Gu Chunhui



Wen Xinyu

Sun K

Wang Dong

Huang Zhenyu

United States Military

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

United States Military

UNITED STATES CYBER COMMAND

24
TWENTY-FOURTH AIR FORCE

10
UNITED STATES TENTH FLEET

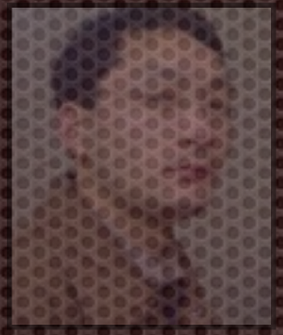
Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Gu Chunhui



Wen Xinyu

Sun

Wang Dong

Huang Zhenyu

United States Military

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

United States Military

UNITED STATES CYBER COMMAND

24 TWENTY-FOURTH AIR FORCE

10 UNITED STATES TENTH FLEET

U.S. ARMY CYBER COMMAND

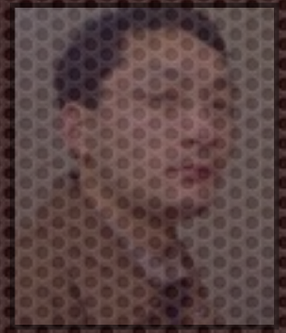
Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Gu Chunhui



Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

FBI CYBER DIVISION

United States Military

UNITED STATES CYBER COMMAND

TWENTY-FOURTH AIR FORCE

UNITED STATES TENTH FLEET

U.S. ARMY CYBER COMMAND

Who Are the Players?

People's Liberation Army

Chen Ping
Codename: cpyy
Unit 61486

3PLA

Unit 61398

Gu Chunhui

Wen Xinyu

Sun Kailiang

Wang Dong

Huang Zhenyu

United States Military

UNITED STATES CYBER COMMAND

24 TWENTY-FOURTH AIR FORCE

10 UNITED STATES TENTH FLEET

U.S. ARMY CYBER COMMAND

FBI CYBER DIVISION

Also: Marine Corps Cyberspace Command


CyberVor
TeslaTeam
Ajax Security Team
RedHack
Syrian Electronic Army
Unit 8200
Iranian Cyber Army

Background

1988 - Morris Worm infects Unix machines worldwide

2006 - Chinese audit of networks finds spyware in classified machines

June 2007 - US Secretary of Defense email hacked

August 2008 - Georgian networks hacked during conflict with Russian military

June 2010 - Stuxnet

April 2007 - Estonian government networks harassed by foreign entity following conflict with Russia

January 2009 - Massive attack against Israel's network. Believed to have been executed by Russian hackers paid for by Hezbollah or Hamas

STUXNET

CLASSIFIED - TOP SECRET
BRIEFING ON STUXNET
SENATE INTELLIGENCE COMMITTEE

Identified

Origin
Most likely USCYBERCOM or Israeli Unit 8200

Affected Machines

Method of Attack
exploits within Windows and Siemens Step7.

Attack

Effect

Attribution: [redacted]

[redacted]

[redacted]

WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WANG DONG
Aliases: Jack Wang, "UglyGorilla"

SUN KAILIANG
Aliases: Sun Kai Liang, Jack Sun

WEN XINYU
Aliases: Wen Xin Yu, "WinXYHappy", "Win_XY", Lao Wen

HUANG ZHENYU
Aliases: Huang Zhen Yu, "hzy_lhx"

GU CHUNHUI
Aliases: Gu Chun Hui, "KandyGoo"

Chen Ping - cpyy

How did we trace a virus to a specific person?

How did we find him?

How do we know he is Chinese military?

```
0000010 0000 0016 0000 0028 0000 0010 0000 0020
0000020 0000 0001 0004 0000 0000 0000 0000 0000
0000030 0000 0000 0000 0010 0000 0000 0000 0204
0000040 0004 8384 0084 c7c8 00c8 4748 0048 e8e9
0000050 00e9 6a69 0069 a8a9 00a9 2828 0028 fdfc
0000060 00fc 1819 0019 9898 0098 d9d8 00d8 5857
0000070 0057 7b7a 007a bab9 00b9 3a3c 003c 8888
0000080 8888 8888 8888 8888 288e be88 8888 8888
0000090 3b83 5788 8888 8888 7667 778e 8828 8888
00000a0 d61f 7abd 8818 8888 467c 585f 8814 8188
00000b0 8b06 e8f7 88aa 8388 8b3b 88f3 88bd e988
00000c0 8a18 880c e841 c988 b328 6871 688e 958b
00000d0 a948 5862 5884 7e81 3788 1ab4 5a84 3eec
00000e0 3d86 dcb8 5cbb 8888 8888 8888 8888 8888
00000f0 8888 8888 8888 8888 8888 8888 8888 0000
0000100 0000 0000 0000 0000 0000 0000 0000 0000
*
0000130 0000 0000 0000 0000 0000 0000 0000
```

CPU - main thread, module kernel32

```
77E7AC72  $ 55              PUSH EBP
77E7AC73  . 8BEC            MOV EBP,ESP
77E7AC75  . FF75 14         PUSH DWORD PTR SS:[EBP+14]
77E7AC78  . FF75 10         PUSH DWORD PTR SS:[EBP+10]
77E7AC7B  . FF75 0C         PUSH DWORD PTR SS:[EBP+C]
77E7AC7E  . FF75 08         PUSH DWORD PTR SS:[EBP+8]
77E7AC81  . 6A FF           PUSH -1
77E7AC83  . E8 9CFFFFFF     CALL kernel32.VirtualAllocEx
77E7AC88  . 5D              POP EBP
77E7AC89  . C2 1000         RETN 10
77E7AC8C  $ 8B4424 04       MOV EAX,DWORD PTR SS:[ESP+4]
77E7AC90  . 85C0            TEST EAX,EAX
77E7AC92  .v0F84 B7010000   JE kernel32.77E7AE4F
77E7AC98  . A8 01           TEST AL,1
77E7AC9A  .^0F85 CAF7FEFF   JNZ kernel32.77E6A46A
77E7ACA0  > C2 0800         RETN 8
77E7ACA3  $-FF25 6413E677   JMP DWORD PTR DS:[<&ntdll.LdrLockLoader>  ntdll.LdrLo
77E7ACA9  $ 6A 28           PUSH 28
77E7ACAB  . 68 283BE877     PUSH kernel32.77E83B28
77E7ACB0  . E8 23F6FFFF     CALL kernel32.77E7A2D8
77E7ACB5  . 33FF            XOR EDI,EDI
77E7ACB7  . 57              PUSH EDI
77E7ACB8  . FF75 08         PUSH DWORD PTR SS:[EBP+8]
77E7ACBB  . E8 CCFFFFFF     CALL kernel32.77E7AC8C
77E7ACC0  . 8945 E4         MOV DWORD PTR SS:[EBP-1C],EAX
77E7ACC3  . 897D E0         MOV DWORD PTR SS:[EBP-20],EDI
77E7ACC6  . 897D DC         MOV DWORD PTR SS:[EBP-24],EDI
77E7ACC9  . 8B5D 10         MOV EBX,DWORD PTR SS:[EBP+10]
77E7ACCC  . D1E3            SHL EBX,1
77E7ACCE  . 397D 08         CMP DWORD PTR SS:[EBP+8],EDI
77E7ACD1  .v75 0F           JNZ SHORT kernel32.77E7ACE2
77E7ACD3    64:A1 18000000  MOV EAX,DWORD PTR FS:[18]
```

```
EBP=0012FF90
Local calls from 77E77F8A, 77E77FBF, ExtendVirtualBuffer+38

kernel32.VirtualAlloc
```

Registers (FPU)

```
EAX 10000000
ECX 0002B000
EDX 77FC306C ntdll.77FC306C
EBX 77E7AC72 kernel32.VirtualAll
ESP 0012FD6C
EBP 0012FF90
ESI 00405B59 ASCII ".text"
EDI 0012FD98 ASCII "PE"

EIP 77E7AC72 kernel32.VirtualAll

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (0000

EFL 00000212 (NO,NB,NE,A,NS,PO,G

ST0 empty +UNORM 17B2 77F51778 7
ST1 empty +UNORM 005E 00000000 0
ST2 empty 3.14759641097577815200
ST3 empty +UNORM 3CDD 77C73CF0 0
ST4 empty 0.00000046968040518 0e
ST5 empty +UNORM 005E 77C77EFE 0
ST6 empty +UNORM 04E4 00000006 0
ST7 empty 0.00000000004492154 0e
               3 2 1 0      E S
FST 0000  Cond 0 0 0 0  Err 0 0
FCW 027F  Prec NEAR,53  Mask
```

Address	Hex dump	ASCII
00400000	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00	MZP.☺...♦.☼. ..
00400010	B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00	¸.......@.→.....
00400020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00400030	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	............☺...
00400040	BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90	‖►.▓▼┤.═!╕☺L═!ÉÉ
00400050	54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73	This program mus
00400060	74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57	t be run under W
00400070	69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00	in32..$7........
00400080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00400090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
004000F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

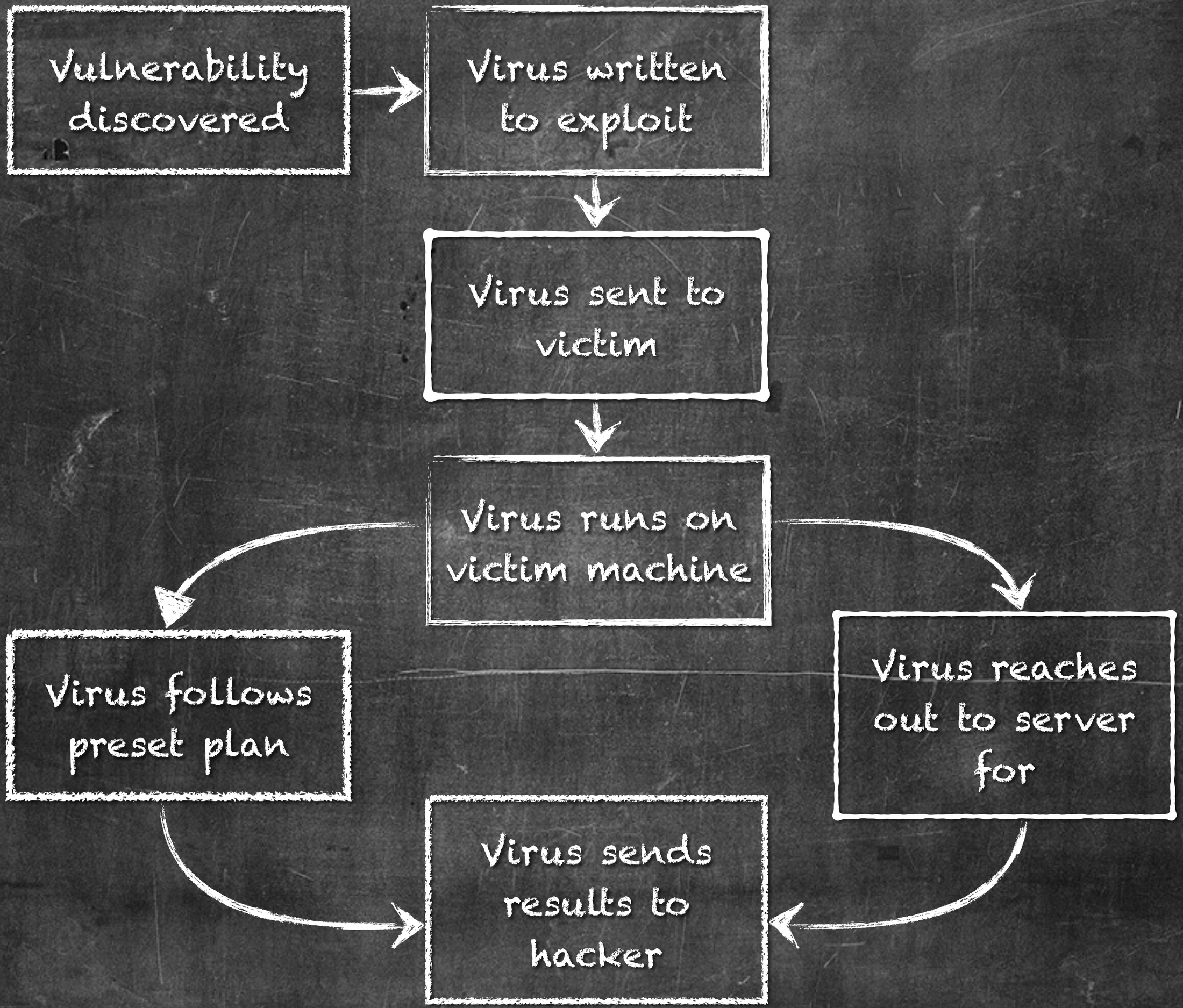
```
0012FD6C  00403298
0012FD70  10000000
0012FD74  0002B000
0012FD78  00003000
0012FD7C  00000040
0012FD80  0002B000
0012FD84  00403564
0012FD88  00000000
0012FD8C  0745F2B8
0012FD90  80DBAE68
0012FD94  00000001
0012FD98  00004550
0012FD9C  0002014C
0012FDA0  44A97E6B
0012FDA4  00000000
0012FDA8  00000000
0012FDAC  210E00E0
```

```
CALL to Virt
Address = 10
Size = 2B00(
AllocationTy
Protect = PF

agent-jz.004(
```

Crackme2:.text

	Text string
0407208	ASCII "Doh!"
04071EC	ASCII "Gimme atleast 4 letters.."
04071E8	ASCII "%d"
04071E0	ASCII "Wee!"
0407198	ASCII "Good Boy!\n If this key is from your keygen u should write an sc
0407208	ASCII "Doh!"
0407188	ASCII "Bad Boy!"
0407180	ASCII "Info"
04070F0	ASCII "KeyGenMe 2 coded by KiTo\n\n Rules: Please, try to NOT patch.\n\
	(Initial CPU selection)
04072A4	ASCII "mscoree.dll"
0407294	ASCII "CorExitProcess"
04076A4	ASCII "<program name unknown>"
04076A0	ASCII "..."
0407684	ASCII "Runtime Error!\n\nProgram: "
0407680	ASCII "\n\n"
0407658	ASCII "Microsoft Visual C++ Runtime Library"
2.00409728	ASCII "C:\\Documents and Settings\\Jason\\Desktop\\Tuts\\Crackmes\\Easy
0407C58	ASCII "user32.dll"
0407C4C	ASCII "MessageBoxA"
0407C3C	ASCII "GetActiveWindow"
0407C28	ASCII "GetLastActivePopup"
0407C0C	ASCII "GetUserObjectInformationA"
0407BF4	ASCII "GetProcessWindowStation"
2.00407DE4	ASCII "Unknown security failure detected!"
S:[EBP-128],C	ASCII "A security error of unknown cause has been detected which has\nc
2.00407D10	ASCII "Buffer overrun detected!"
S:[EBP-128],C	ASCII "A buffer overrun has been detected which has corrupted the progr
04076A4	ASCII "<program name unknown>"
04076A0	ASCII "..."
2.00407680	ASCII "\n\n"
0407C64	ASCII "Program: "
0407658	ASCII "Microsoft Visual C++ Runtime Library"


Vulnerability discovered
Virus written to exploit
Virus sent to victim
Virus runs on victim machine
Virus follows preset plan
Virus reaches out to server for
Virus sends results to hacker

Crackme2:.text

	Text string
0407208	ASCII "Doh!"
04071EC	ASCII "Gimme atleast 4 letters.."
04071E8	ASCII "%d"
04071E0	ASCII "Wee!"
0407198	ASCII "Good Boy!\n If this key is from your keygen u should write an sc
0407208	ASCII "Doh!"
0407188	ASCII "Bad Boy!"
0407180	ASCII "Info"
04070F0	ASCII "KeyGenMe 2 coded by KiTo\n\n Rules: Please, try to NOT patch.\n\
	(Initial CPU selection)
04072A4	ASCII "mscoree.dll"
0407294	ASCII "CorExitProcess"
04076A4	ASCII "<program name unknown>"
04076A0	ASCII "..."
0407684	ASCII "Runtime Error!\n\nProgram: "
0407680	ASCII "\n\n"
0407658	ASCII "Microsoft Visual C++ Runtime Library"
2.00409728	ASCII "C:\\Documents and Settings\\Jason\\Desktop\\Tuts\\Crackmes\\Easy
0407C58	ASCII "user32.dll"
0407C4C	ASCII "MessageBoxA"
0407C3C	ASCII "GetActiveWindow"
0407C28	ASCII "GetLastActivePopup"
0407C0C	ASCII "GetUserObjectInformationA"
0407BF4	ASCII "GetProcessWindowStation"
2.00407DE4	ASCII "Unknown security failure detected!"
S:[EBP-128],C	ASCII "A security error of unknown cause has been detected which has\nc
2.00407D10	ASCII "Buffer overrun detected!"
S:[EBP-128],C	ASCII "A buffer overrun has been detected which has corrupted the progr
04076A4	ASCII "<program name unknown>"
04076A0	ASCII "..."
2.00407680	ASCII "\n\n"
0407C64	ASCII "Program: "
0407658	ASCII "Microsoft Visual C++ Runtime Library"

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.0.12	192.228.79.201	DNS	Standard query A www.mit.edu
2	0.000307	10.1.0.12	192.228.79.201	DNS	Standard query NS <Root>
3	0.070425	192.228.79.201	10.1.0.12	DNS	Standard query response
4	0.071715	10.1.0.12	192.41.162.32	DNS	Standard query A www.mit.edu
5	0.075844	192.228.79.201	10.1.0.12	DNS	Standard query response NS G.ROOT-SERVERS.NET NS H.ROOT-SERV
6	0.135333	192.41.162.32	10.1.0.12	DNS	Standard query response
7	0.135885	10.1.0.12	18.71.0.151	DNS	Standard query A www.mit.edu
8	0.224063	18.71.0.151	10.1.0.12	DNS	Standard query response A 18.7.22.83
9	0.226098	10.1.0.12	18.72.0.3	DNS	Standard query AAAA www.mit.edu
10	0.312355	18.72.0.3	10.1.0.12	DNS	Standard query response
11	0.313446	10.1.0.12	18.70.0.160	DNS	Standard query MX www.mit.edu
12	0.399408	18.70.0.160	10.1.0.12	DNS	Standard query response

C2 DOMAIN	REGISTRANT EMAIL ADDRESS
hgcurtain.com	andre.poli@gmail.com
cultivr.com	beth.purcell@gmail.com
tensins.net	burnyice@163.com
decipherment.net	charles.kenta@gmail.com
konamidata.com	charles.kenta@gmail.com
cbssrayli.com	chenhaiwei1977@163.com
windowsupdote.net	cl_flywind@sohu.com
ctable.org	cpyy.chen@gmail.com
gamemuster.com	cpyy.chen@gmail.com
kyoceras.net	cpyy.chen@gmail.com
nestlere.com	cpyy.chen@gmail.com
raylitoday.com	cpyy.chen@gmail.com
renewgis.com	cpyy.chen@gmail.com
siseau.com	cpyy@qq.com
bmwauto.org	cpyy@sina.com

cpyy's personal blog on 163.com

Found on cpyy's online activity

"On the XCar forum, cpyy.chen used a subforum called Polo (hacker slang for "Volkswagen cars") to communicate with other users linxder, peggycat, "naturally do not understand romance" (天生不懂浪漫), "a wolf" (一只大灰狼), "large tile" (大瓦片), "winter" (冬夜), "chunni" (春妮), papaya, kukuhaha, Cranbing, "dusty sub" (多尘子), z11829, "ice star harbor" (冰星港), "polytechnic aberdeen" (理工仔), "I love pineapplepie" (我爱菠罗派), and "she's distant" in 2007. although superficially the discussion is about cars, there is a repeated word in the text, "milk yellow package" or "custard package" or "yoke package" (奶黄包). this could be a hacker slang word, but it is unclear as to the definition. the conversation alludes to linxder being the "teacher" or "landlord" and the other aforementioned users are his "students". linxder references how he has "found jobs" for them. It is possible that this is a reference to hacking jobs wrapped up in car metaphors."

Source: CrowdStrike Intelligence Report

How Do We Link Attacks To Each Other?

How to Link Attacks

Similar binary

- Identical hashes
- Similar code snippets
- Embedded strings

Method of attack

- Attack vector (phishing, watering hole, SQL injection)
- Exploit (CVE 2014-0160)
- C2 Domain

Recommended Reading

- Bartlett, Jonathon. *Programming from the Ground Up.* Copyright 2003. http://savannah.nongnu.org/projects/pgubook

- CrowdStrike Global Intelligence Team. *CrowdStrike Intelligence Report: Putter Panda*. CrowdStrike. http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

- Hall, Justin. *Still in Hiding*. CBTS Advanced Cybersecurity Blog. http://cbts.net/Education-Events/CBTS-Blog/Still-in-Hiding

- Hutchins, Eric M. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

- R4ndom. *R4ndom's Beginning Reverse Engineering Tutorials*. The Legend of Random. http://thelegendofrandom.com/blog/sample-page