xStart when you’re ready
Uncovering a threat actor targeting China

John Southworth
January 2021

About me

John Southworth
Senior Threat Intelligence Analyst

PwC UK

- Tracking threat actors in the Asia-Pacific region:
  - North Korea-based
  - China-based
- Malware reverse engineering
- Infrastructure tracking
- Amateur jazz pianist

@BitsOfBinary

bitsofbinary

BitsOfBinary

Aims of the talk

- How were these campaigns found?
- xStart analysis
  - Malware analysis
  - Configuration decoding
  - Tracking the malware family
- Infrastructure tracking
- Decoy document analysis + targeting
- Points on attribution
- Further research

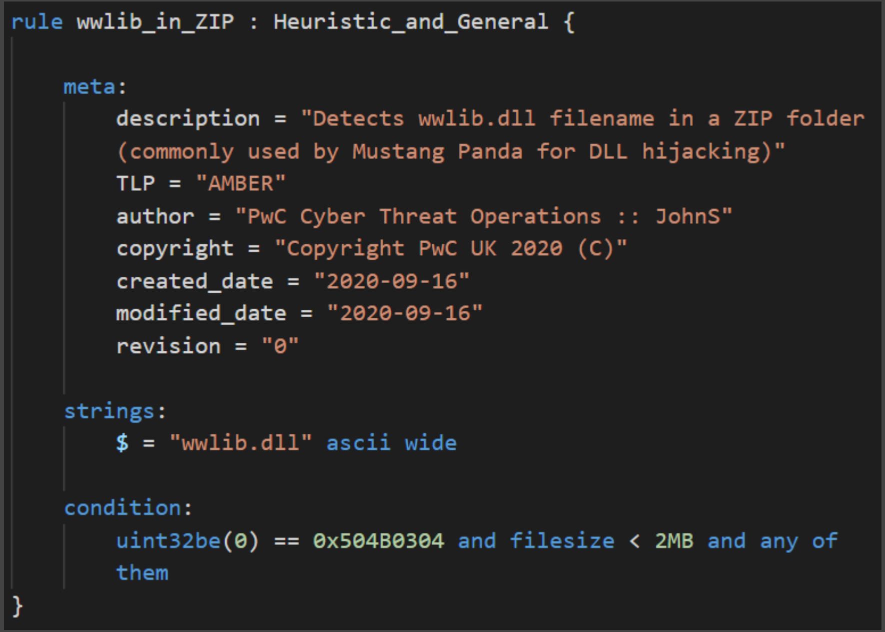
Indicators + Yara rules + scripts:

https://github.com/PwCUK-CTO/SANSCTISummit2021-xStart

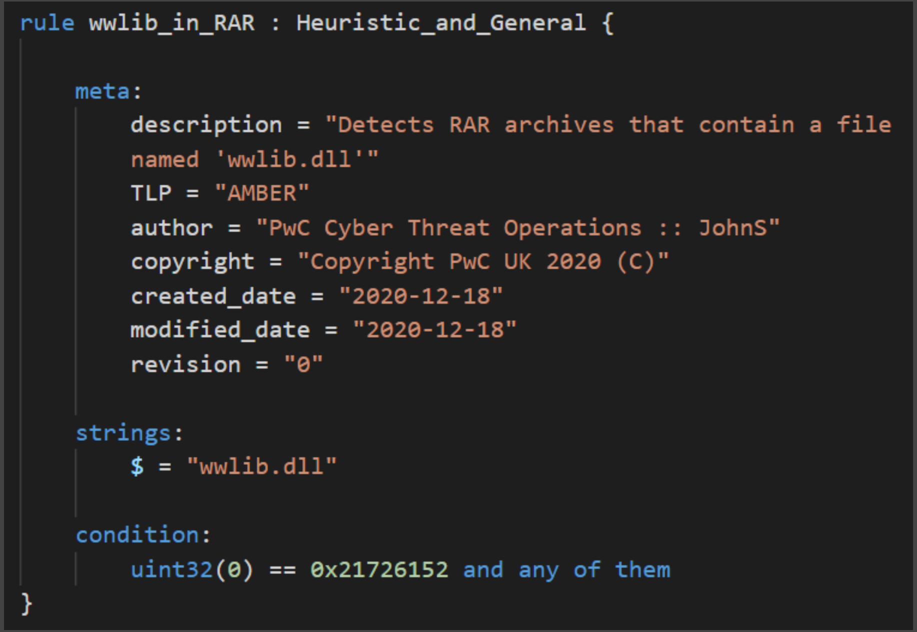
Hunting for samples: DLL search order hijacking

- APTs have been using ‘`wwlib.dll`’ to DLL search order hijack into ‘`WinWord.exe`’
- Benefit: renaming ‘`WinWord.exe`’ can be used to make it look like Word document
- Extra steps:
  - Give ‘`wwlib.dll`’ the “Hidden” file attribute
  - Right to left override ‘`WinWord.exe`’ to make it look like it has a ‘`.doc`’ extension
- Threat actors using this technique in 2020:
  - Mustang Panda/Red Delta
  - Ocean Lotus/APT32

Hunting for samples: YARA rules



```
rule wwlib_in_ZIP : Heuristic_and_General {

    meta:
        description = "Detects wwlib.dll filename in a ZIP folder
        (commonly used by Mustang Panda for DLL hijacking)"
        TLP = "AMBER"
        author = "PwC Cyber Threat Operations :: JohnS"
        copyright = "Copyright PwC UK 2020 (C)"
        created_date = "2020-09-16"
        modified_date = "2020-09-16"
        revision = "0"

    strings:
        $ = "wwlib.dll" ascii wide

    condition:
        uint32be(0) == 0x504B0304 and filesize < 2MB and any of
        them
}
```



```
rule wwlib_in_RAR : Heuristic_and_General {

    meta:
        description = "Detects RAR archives that contain a file
        named 'wwlib.dll'"
        TLP = "AMBER"
        author = "PwC Cyber Threat Operations :: JohnS"
        copyright = "Copyright PwC UK 2020 (C)"
        created_date = "2020-12-18"
        modified_date = "2020-12-18"
        revision = "0"

    strings:
        $ = "wwlib.dll"

    condition:
        uint32(0) == 0x21726152 and any of them
}
```

Finding xStart

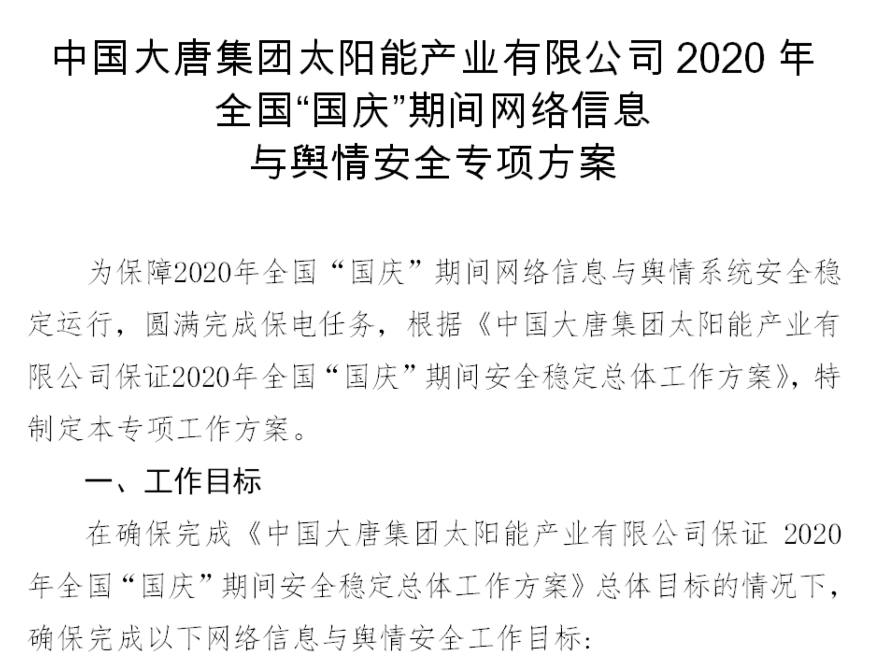
- The ‘`wwlib.dll`’ ZIP YARA rule picked up the following sample:

Filename	`2020年全国“国庆”期间网络信息与舆情安全专项方案.zip`
Translated filename	`A special plan for network information and public opinion security during the national "National Day" in 2020.zip`
SHA256	`60b33385519592a3ae48bd82767cbc617fd62fb2ee7fed83b4aa6fe3c9d79420`
Last modified	`2020-09-21 17:50:18`

- This is where the investigation begins….

Introducing xStart

- xStart is a shellcode loader that also drops and opens a decoy document to be displayed to the victim
- The shellcode will attempt to download and execute the Cobalt Strike Beacon module via HTTP
- Shellcode is injected into the following process (spawned as child processes):
    - `rundll32.exe`
    - `explorer.exe`
    - `WinWord.exe`



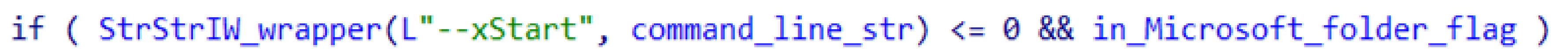
中国大唐集团太阳能产业有限公司 2020 年
全国“国庆”期间网络信息
与舆情安全专项方案

为保障2020年全国“国庆”期间网络信息与舆情系统安全稳定运行，圆满完成保电任务，根据《中国大唐集团太阳能产业有限公司保证2020年全国“国庆”期间安全稳定总体工作方案》，特制定本专项工作方案。

一、工作目标

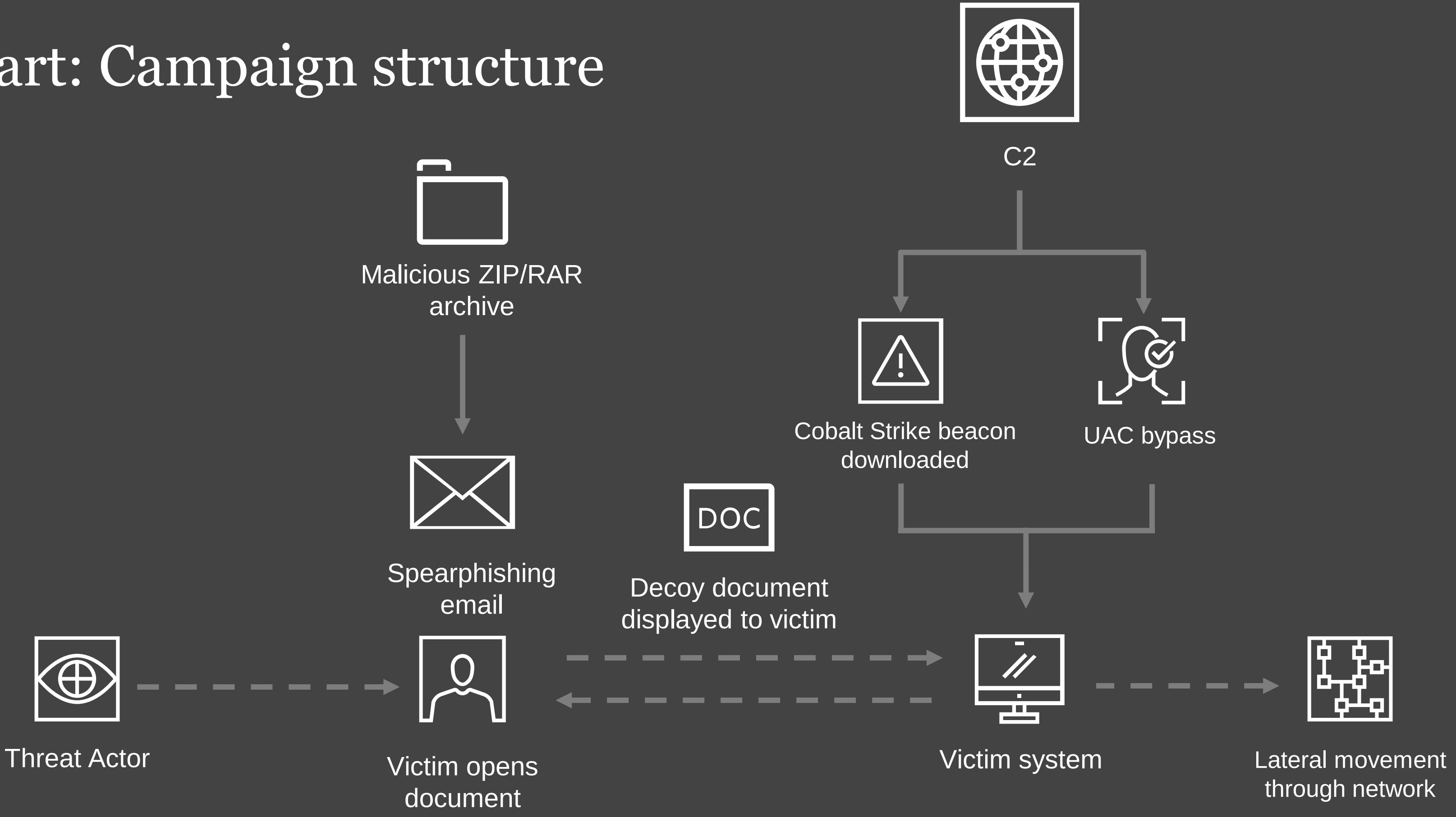
在确保完成《中国大唐集团太阳能产业有限公司保证 2020 年全国“国庆”期间安全稳定总体工作方案》总体目标的情况下，确保完成以下网络信息与舆情安全工作目标：

Title includes: “`China Datang Group Solar Energy Industry Co., Ltd. 2020`”



```
if ( StrStrIW_wrapper(L"--xStart", command_line_str) <= 0 && in_Microsoft_folder_flag )
```

xStart: Campaign structure



C2

Malicious ZIP/RAR archive

Cobalt Strike beacon downloaded

UAC bypass

Spearphishing email

Decoy document displayed to victim

Threat Actor

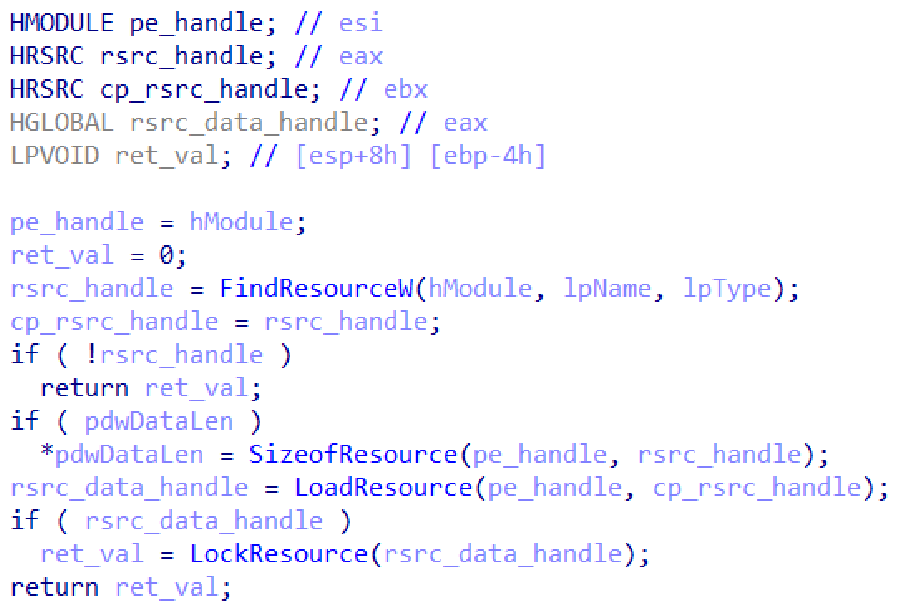
Victim opens document

Victim system

Lateral movement through network

xStart: Encrypted resources

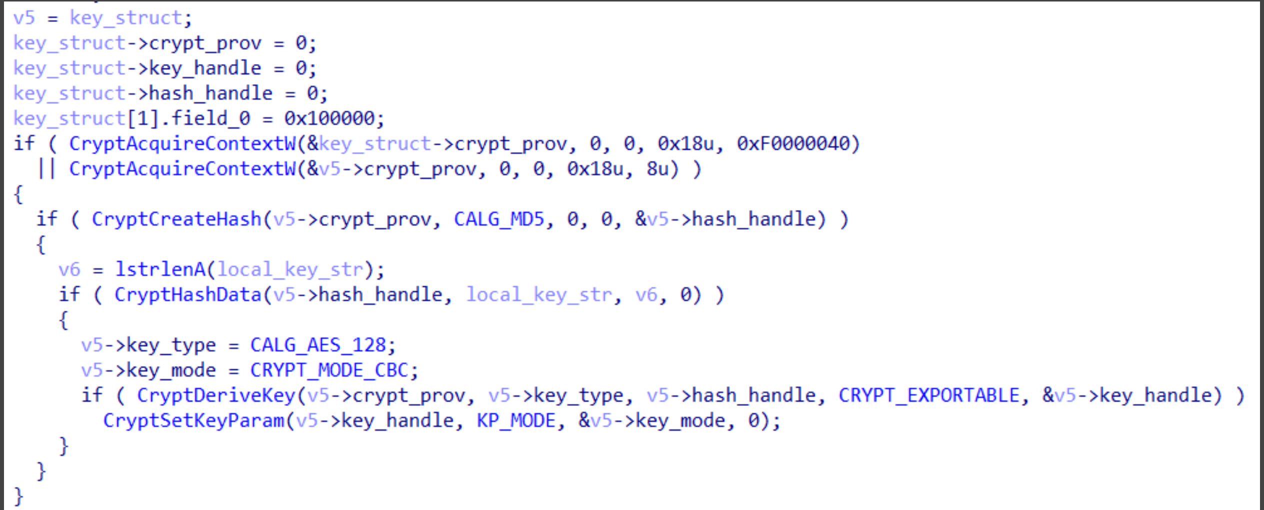
- Most samples have two encrypted PE resources:
    - `MKV` - decoy document
    - `MP4` - shellcode (downloader)
- The decoy document is written to disk (and the original EXE and DLL deleted).
- The (decoded) shellcode is in memory only.



```
HMODULE pe_handle; // esi
HRSRC rsrc_handle; // eax
HRSRC cp_rsrc_handle; // ebx
HGLOBAL rsrc_data_handle; // eax
LPVOID ret_val; // [esp+8h] [ebp-4h]

pe_handle = hModule;
ret_val = 0;
rsrc_handle = FindResourceW(hModule, lpName, lpType);
cp_rsrc_handle = rsrc_handle;
if ( !rsrc_handle )
  return ret_val;
if ( pdwDataLen )
  *pdwDataLen = SizeofResource(pe_handle, rsrc_handle);
rsrc_data_handle = LoadResource(pe_handle, cp_rsrc_handle);
if ( rsrc_data_handle )
  ret_val = LockResource(rsrc_data_handle);
return ret_val;
```

xStart: Cryptography Routine

- The PE resources are encrypted with AES-128 in CBC mode.
- The key is stored as a plaintext string, which is MD5 hashed and then passed to ‘`CryptDeriveKey`’.



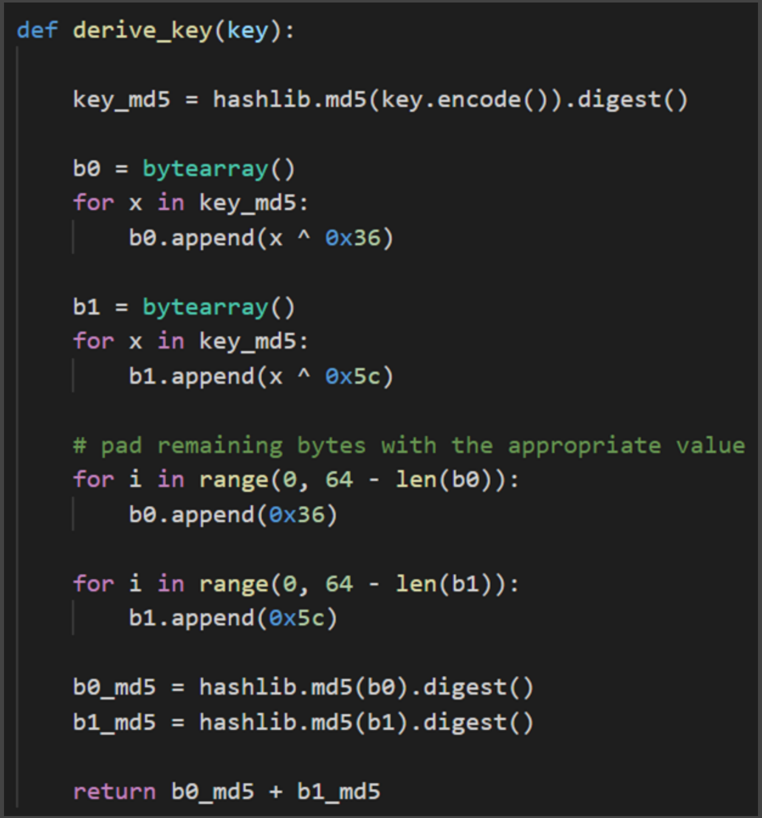
```
v5 = key_struct;
key_struct->crypt_prov = 0;
key_struct->key_handle = 0;
key_struct->hash_handle = 0;
key_struct[1].field_0 = 0x100000;
if ( CryptAcquireContextW(&key_struct->crypt_prov, 0, 0, 0x18u, 0xF0000040)
  || CryptAcquireContextW(&v5->crypt_prov, 0, 0, 0x18u, 8u) )
{
  if ( CryptCreateHash(v5->crypt_prov, CALG_MD5, 0, 0, &v5->hash_handle) )
  {
    v6 = lstrlenA(local_key_str);
    if ( CryptHashData(v5->hash_handle, local_key_str, v6, 0) )
    {
      v5->key_type = CALG_AES_128;
      v5->key_mode = CRYPT_MODE_CBC;
      if ( CryptDeriveKey(v5->crypt_prov, v5->key_type, v5->hash_handle, CRYPT_EXPORTABLE, &v5->key_handle) )
        CryptSetKeyParam(v5->key_handle, KP_MODE, &v5->key_mode, 0);
    }
  }
}
```

xStart: Auto-config extractor

- This is enough information to automate a method of automatically decrypting xStart PE resources.
- Language of choice: Python 3
- Goals:
  - Parse AES-128 key
  - Load and decode PE resources
  - Parse IoCs
- Packages used:
  - `pycryptodome`
  - `pefile`

- Challenges:
  - False positives parsing key
  - `CryptDeriveKey` implementation

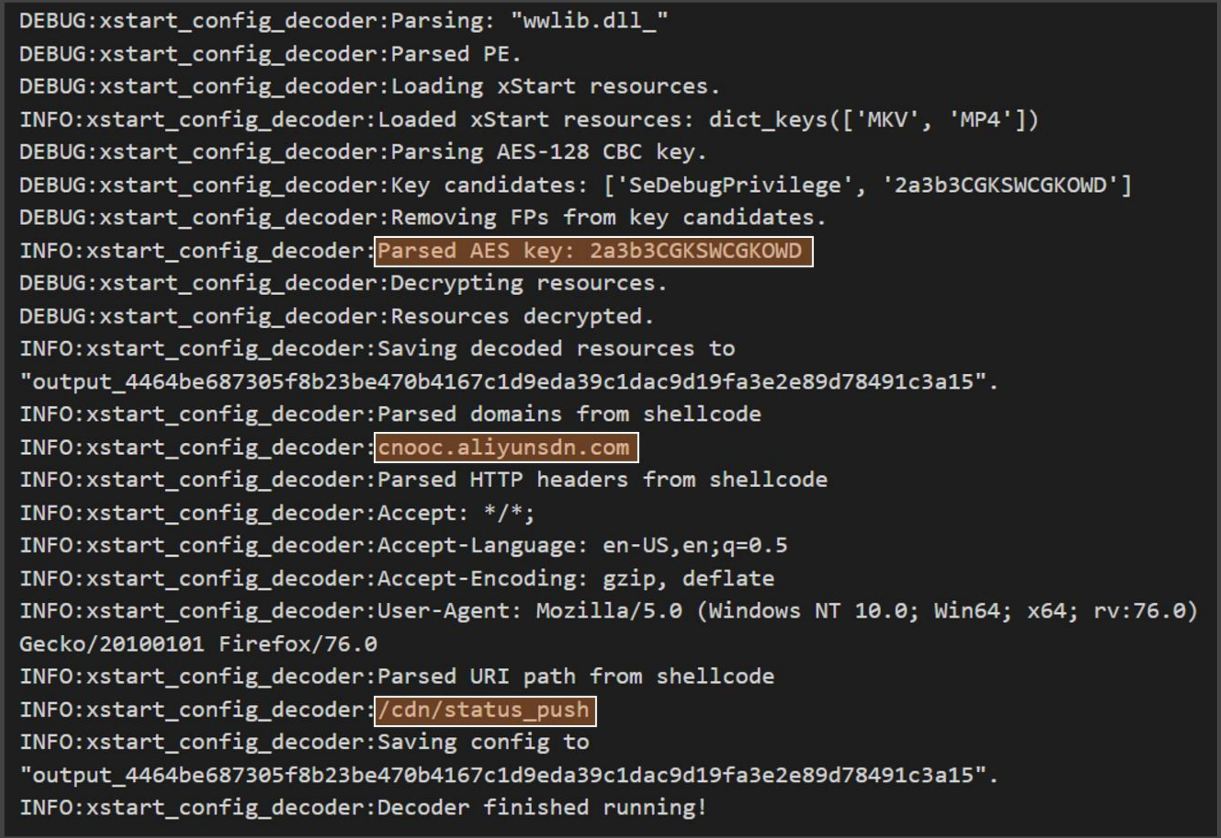
xStart: CryptDeriveKey Python 3 implementation



```python
def derive_key(key):

    key_md5 = hashlib.md5(key.encode()).digest()

    b0 = bytearray()
    for x in key_md5:
        b0.append(x ^ 0x36)

    b1 = bytearray()
    for x in key_md5:
        b1.append(x ^ 0x5c)

    # pad remaining bytes with the appropriate value
    for i in range(0, 64 - len(b0)):
        b0.append(0x36)

    for i in range(0, 64 - len(b1)):
        b1.append(0x5c)

    b0_md5 = hashlib.md5(b0).digest()
    b1_md5 = hashlib.md5(b1).digest()

    return b0_md5 + b1_md5
```

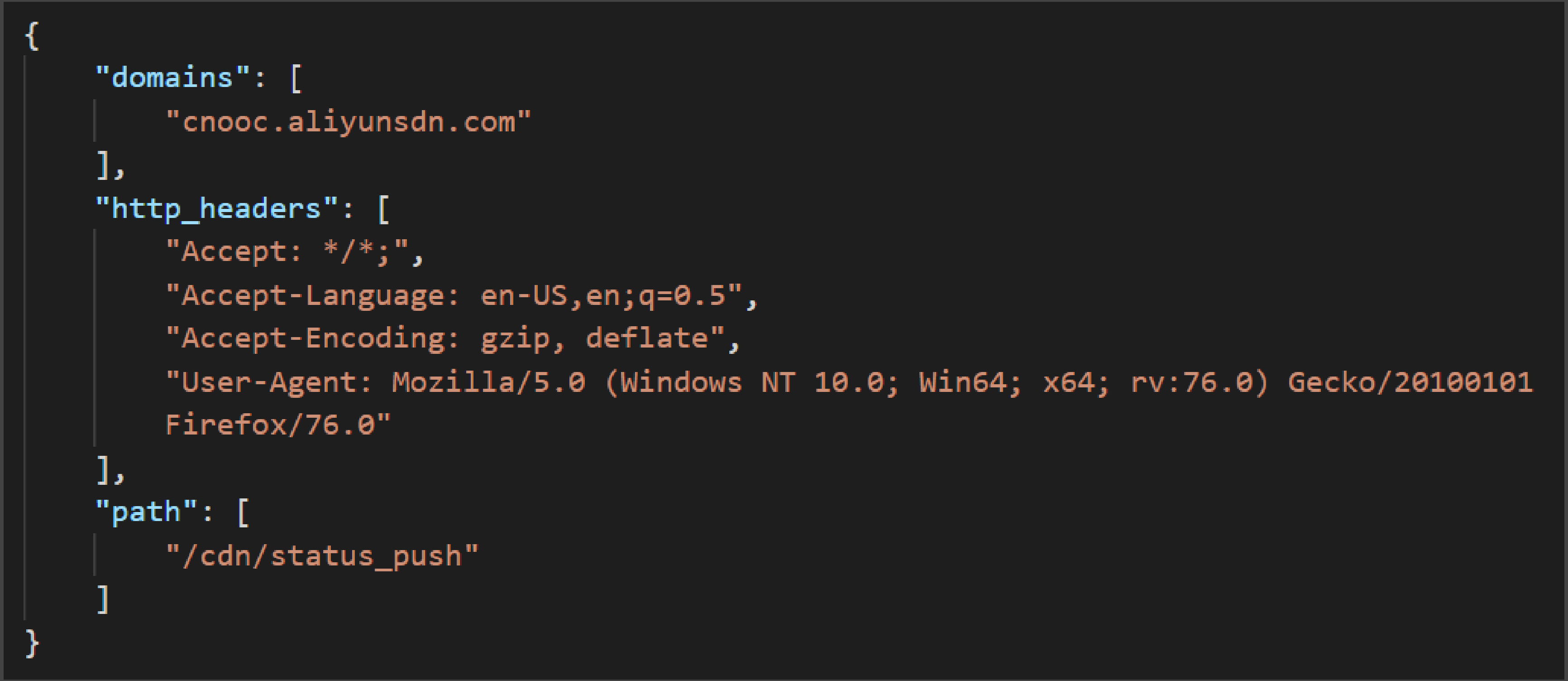
Reference:
https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/flareon2016/challenge2-solution.pdf

xStart: Config extractor example run - logging



```
DEBUG:xstart_config_decoder:Parsing: "wwlib.dll_"
DEBUG:xstart_config_decoder:Parsed PE.
DEBUG:xstart_config_decoder:Loading xStart resources.
INFO:xstart_config_decoder:Loaded xStart resources: dict_keys(['MKV', 'MP4'])
DEBUG:xstart_config_decoder:Parsing AES-128 CBC key.
DEBUG:xstart_config_decoder:Key candidates: ['SeDebugPrivilege', '2a3b3CGKSWCGKOWD']
DEBUG:xstart_config_decoder:Removing FPs from key candidates.
INFO:xstart_config_decoder:Parsed AES key: 2a3b3CGKSWCGKOWD
DEBUG:xstart_config_decoder:Decrypting resources.
DEBUG:xstart_config_decoder:Resources decrypted.
INFO:xstart_config_decoder:Saving decoded resources to
"output_4464be687305f8b23be470b4167c1d9eda39c1dac9d19fa3e2e89d78491c3a15".
INFO:xstart_config_decoder:Parsed domains from shellcode
INFO:xstart_config_decoder:cnooc.aliyunsdn.com
INFO:xstart_config_decoder:Parsed HTTP headers from shellcode
INFO:xstart_config_decoder:Accept: */*;
INFO:xstart_config_decoder:Accept-Language: en-US,en;q=0.5
INFO:xstart_config_decoder:Accept-Encoding: gzip, deflate
INFO:xstart_config_decoder:User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
INFO:xstart_config_decoder:Parsed URI path from shellcode
INFO:xstart_config_decoder:/cdn/status_push
INFO:xstart_config_decoder:Saving config to
"output_4464be687305f8b23be470b4167c1d9eda39c1dac9d19fa3e2e89d78491c3a15".
INFO:xstart_config_decoder:Decoder finished running!
```

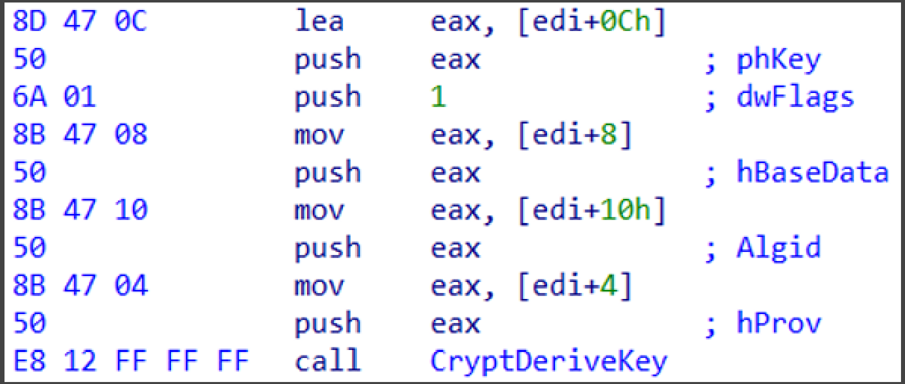
xStart: Config extractor example run - config



```
{
    "domains": [
        "cnooc.aliyunsdn.com"
    ],
    "http_headers": [
        "Accept: */*;",
        "Accept-Language: en-US,en;q=0.5",
        "Accept-Encoding: gzip, deflate",
        "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0"
    ],
    "path": [
        "/cdn/status_push"
    ]
}
```

xStart: Finding more samples - YARA ideas

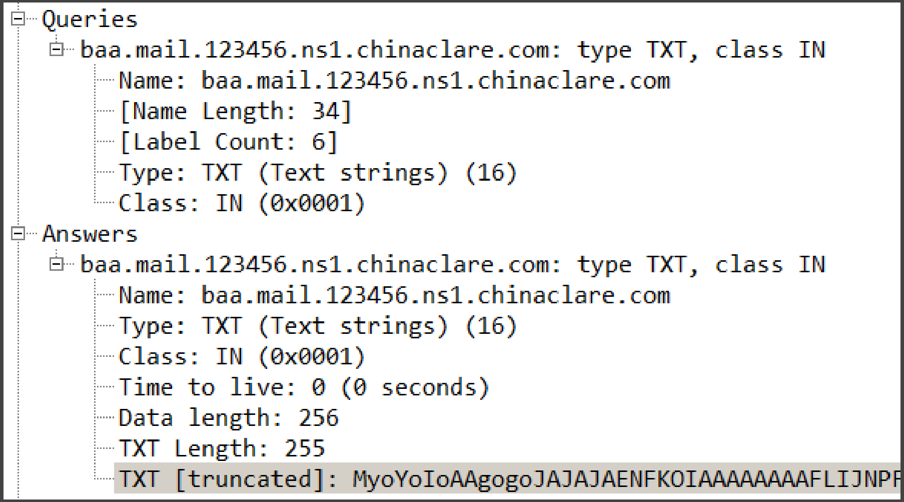
- Strings:
  - “`%s --xStart`”
  - “`Unit_AES        Unit_Func`” (tab in the middle, i.e. the `0x09` character)
- PE metadata
  - Import hash (imphash)
  - PE resource names (`MKV`, `MP4`)
- Code:
  - Unique structure offsets before calls, such as ‘`[edi+8]`’



```
8D 47 0C        lea     eax, [edi+0Ch]
50              push    eax              ; phKey
6A 01           push    1                ; dwFlags
8B 47 08        mov     eax, [edi+8]
50              push    eax              ; hBaseData
8B 47 10        mov     eax, [edi+10h]
50              push    eax              ; Algid
8B 47 04        mov     eax, [edi+4]
50              push    eax              ; hProv
E8 12 FF FF FF  call    CryptDeriveKey
```

xStart: Finding more samples - some facts

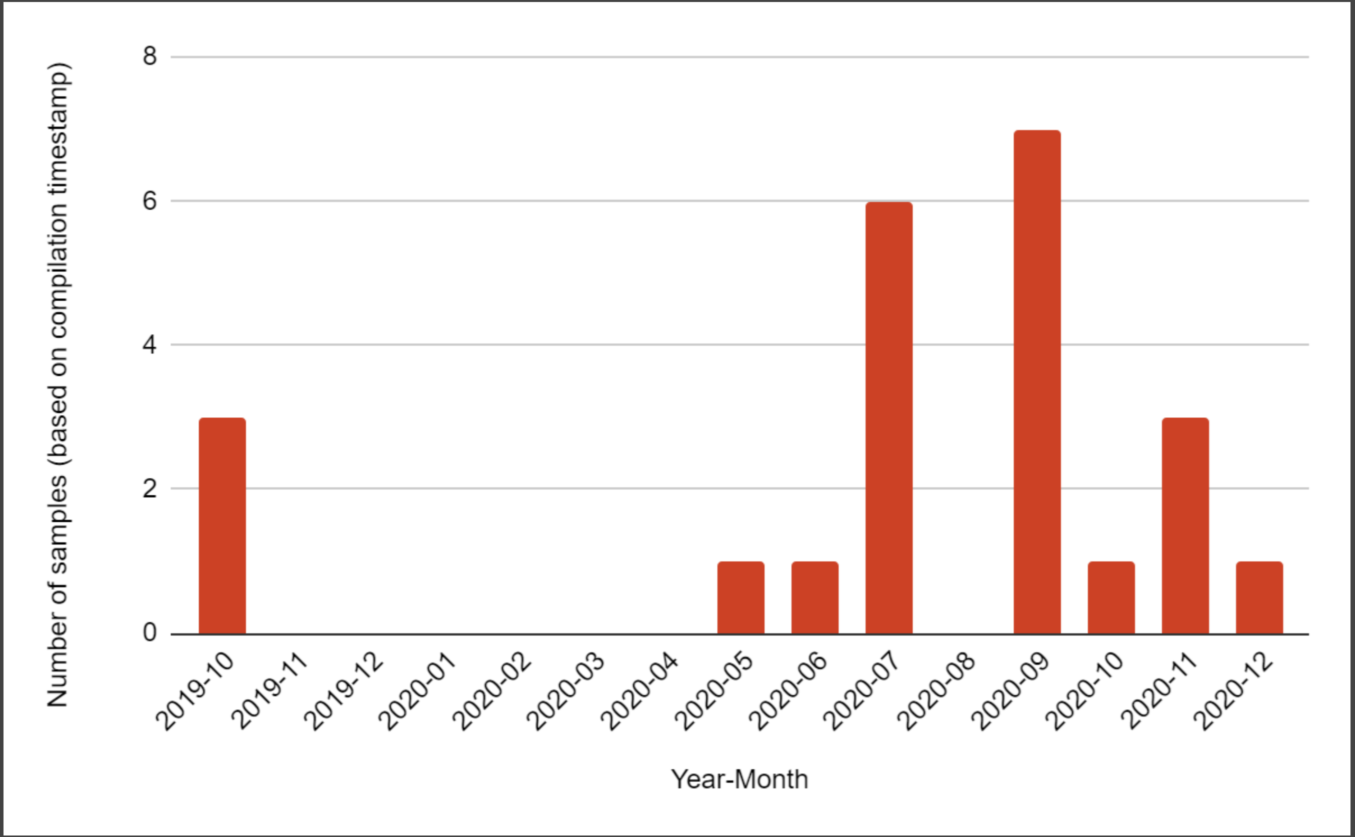
- xStart has been used since at least October 2019
- Other DLLs used for search order hijacking:
  - `Qt5Gui.dll`
  - `goopdate.dll`
- One variant’s shellcode uses DNS instead of HTTP to download the Cobalt Strike payload



```
⊟ Queries
   ⊟ baa.mail.123456.ns1.chinaclare.com: type TXT, class IN
        Name: baa.mail.123456.ns1.chinaclare.com
        [Name Length: 34]
        [Label Count: 6]
        Type: TXT (Text strings) (16)
        Class: IN (0x0001)
⊟ Answers
   ⊟ baa.mail.123456.ns1.chinaclare.com: type TXT, class IN
        Name: baa.mail.123456.ns1.chinaclare.com
        Type: TXT (Text strings) (16)
        Class: IN (0x0001)
        Time to live: 0 (0 seconds)
        Data length: 256
        TXT Length: 255
        TXT [truncated]: MyoYoIoAAgogoJAJAJAENFKOIAAAAAAAAFLIJNPF
```

Packets from DNS shellcode variant

xStart: Compile timestamp graph



xStart: Infrastructure

- CDN/cloud service provider spoofing
  - `aliyunsdn[.]com (Alibaba)`
  - `didiyuncdn[.]com`
- Financial services spoofing
  - `chinaclare[.]com (CSDC)`
- IP infrastructure:
  - Choopa
  - Alibaba
- IPs and domains are reused for xStart campaigns

Alibaba Group
阿里巴巴集团

中国结算
CSDC

choopa.com

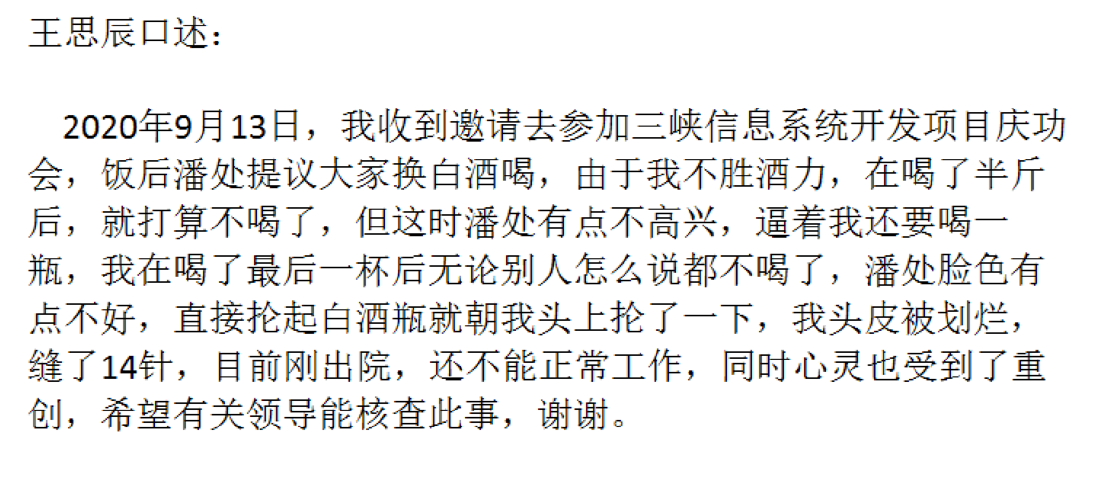
xStart: Finding more infrastructure

- Check further subdomains:
  - `casicloud[.]aliyunsdn[.]com`
  - `hangzhou[.]didiyuncdn[.]com`
  - `hubei[.]didiyuncdn[.]com`
- Domain resolutions to known IPs:
  - `me[.]microsofts-update[.]com`
  - `safe[.]tang-cloud[.]com`
  - `china-inv[.]org`

Regex pattern to consider:
`[a-z]{3,4}yun[cs]dn`

xStart: Decoy document example 1

- Complaint form from an employee
- Mentions “`Three Gorges Information System Development Project`”
- Likely target sector:
  - Energy
  - Utilities



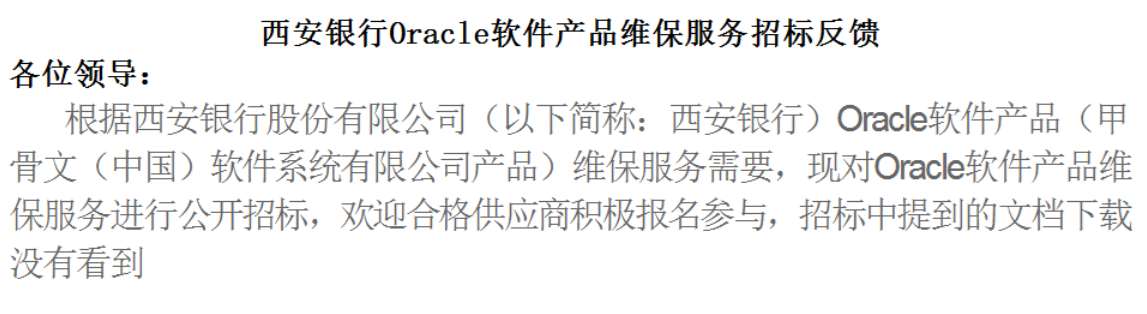
王思辰口述:

2020年9月13日，我收到邀请去参加三峡信息系统开发项目庆功会，饭后潘处提议大家换白酒喝，由于我不胜酒力，在喝了半斤后，就打算不喝了，但这时潘处有点不高兴，逼着我还要喝一瓶，我在喝了最后一杯后无论别人怎么说都不喝了，潘处脸色有点不好，直接抡起白酒瓶就朝我头上抡了一下，我头皮被划烂，缝了14针，目前刚出院，还不能正常工作，同时心灵也受到了重创，希望有关领导能核查此事，谢谢。

Document dropped by:
`0bff0d4bcbd5545072b5f8f87d0982cbcdfc66021a2bad486fa2111bf68be60d`

xStart: Decoy document example 2

- Titled “Feedback from Xi'an Bank Oracle Software Product Maintenance Service Bidding”
- Looks like an invitation to bid for a project
- Likely target sector(s):
  - Financial services
  - Technology



西安银行Oracle软件产品维保服务招标反馈

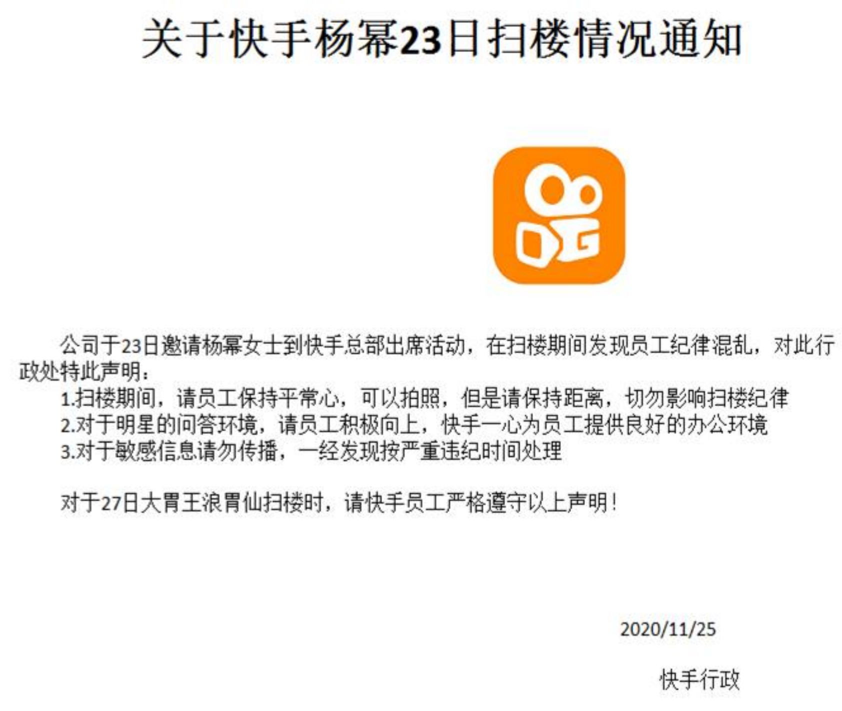
各位领导：

根据西安银行股份有限公司（以下简称：西安银行）Oracle软件产品（甲骨文（中国）软件系统有限公司产品）维保服务需要，现对Oracle软件产品维保服务进行公开招标，欢迎合格供应商积极报名参与，招标中提到的文档下载没有看到

Document dropped by:
`b64a4cd485f72e9ce1503b50cd2b5f9f0d8e08d7616543e4acfa559a9b05af34`

xStart: Decoy document example 3

- Describing a “building sweep” of the company Kuaishou
- Talking about the visit of the Chinese celebrity Yang Mi
- Likely target sector:
    - Technology



关于快手杨幂23日扫楼情况通知

公司于23日邀请杨幂女士到快手总部出席活动，在扫楼期间发现员工纪律混乱，对此行政处特此声明：

1.扫楼期间，请员工保持平常心，可以拍照，但是请保持距离，切勿影响扫楼纪律
2.对于明星的问答环境，请员工积极向上，快手一心为员工提供良好的办公环境
3.对于敏感信息请勿传播，一经发现按严重违纪时间处理

对于27日大胃王浪胃仙扫楼时，请快手员工严格遵守以上声明！

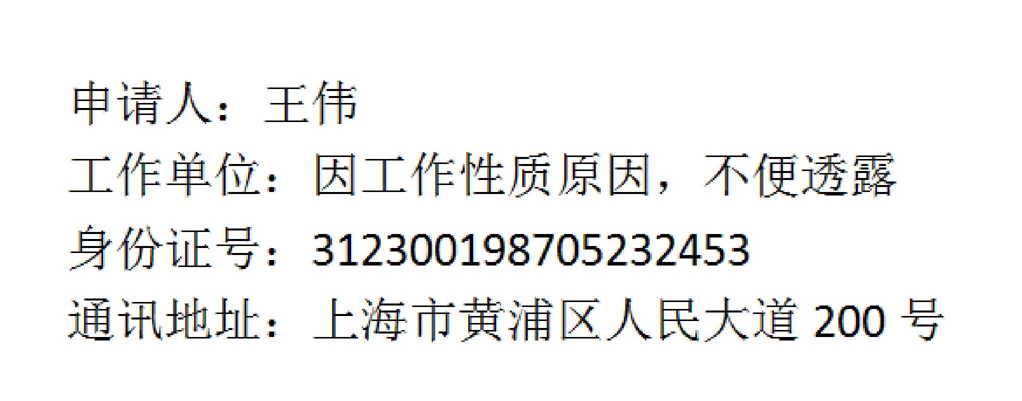
2020/11/25

快手行政

Document dropped by:
`e7357b82378dd30074b15b69f6b729c29d4d0b666a345e4739e8d6414ab47fe5`

xStart: Decoy document example 4

- Job application form for “Wang Wei”
- Gives the address of Shanghai's municipal government headquarters building
- Realistic probability target sector:
  - Government



申请人：王伟

工作单位：因工作性质原因，不便透露

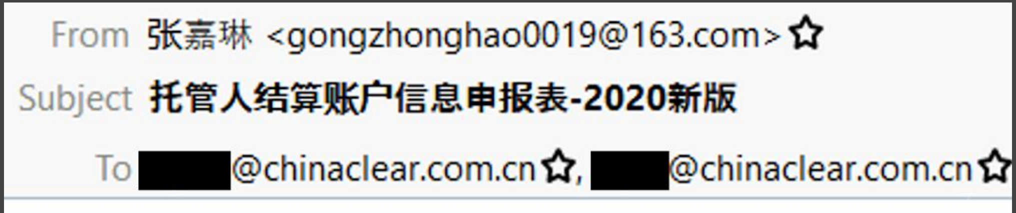
身份证号：312300198705232453

通讯地址：上海市黄浦区人民大道 200 号

Document dropped by:
`f38b65df5a1ec605c189e6b586455ff444b48a69b3f13bb62550e9e57852cf05`

xStart: Phishing email

- Attached ZIP file with xStart sample and renamed ‘`WinWord.exe`’
- Targeting email addresses of ChinaClear (also known as China Securities Depository and Clearing Corporation)



From 张嘉琳 <gongzhonghao0019@163.com>

Subject 托管人结算账户信息申报表-2020新版

To [redacted]@chinaclear.com.cn, [redacted]@chinaclear.com.cn

SHA256	7096e5e611001ab28892adfd1dbfc246 8067f1348c219b896e18afa7e9f874e6
File type	Email
File size	610,269 bytes
Received	2020-09-23 11:45:18 +0800 (CST)

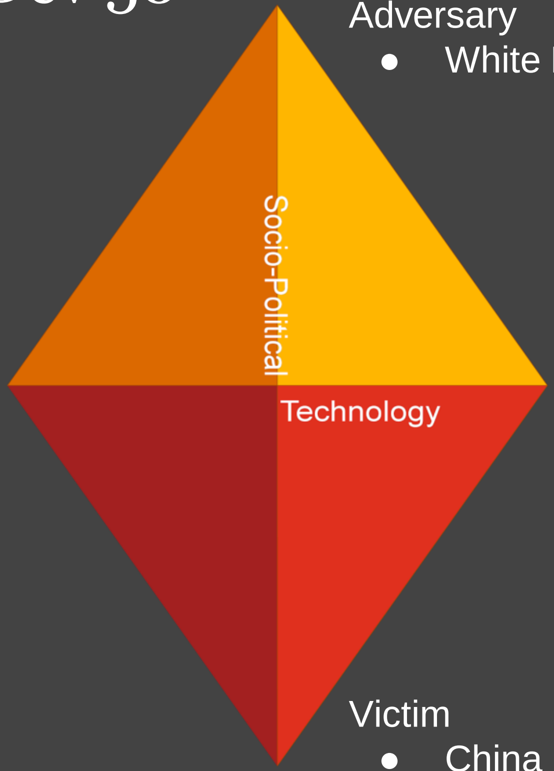
xStart: Targeting summary

- Likely target sectors:
  - Financial services
  - Insurance
  - Energy
  - Utilities
  - Technology
- Realistic probability target sectors
  - Government
- Lures observed written in Mandarin
- Most samples uploaded from China

xStart: Attribution (or lack thereof)

- We haven’t observed enough evidence to connect this activity to any known threat actors
- Bias could lead to OceanLotus attribution, but not enough evidence to rule out the alternative hypothesis (i.e. that it’s an unknown threat actor)
- Points to consider for attribution:
  - **Capability** - Cobalt Strike and ‘`wwlib.dll`’ search order hijacking
  - **Infrastructure** - themed around regions/technology used in China
  - **Targeting** - organisations in China in financial services, technology, energy/utilities

Threat actor: White Dev 50



Adversary

- White Dev 50

Infrastructure

- Aliyun/Alibaba CDN spoofing
- China financial services spoofing
- Choopa and Alibaba hosting

Capability

- xStart dropper
- Cobalt Strike
- DLL search order hijacking

Victim

- China
- Financial Services
- Energy/Utilities
- Technology

Thoughts on endpoint detection

- DLL search order hijacking:
  - Look for DLLs being created in/loaded from unconventional paths
- Code injection
  - Check if processes such as ‘`rundll32`’ should be making network connections
- YARA rules
  - Scan compressed email attachments with YARA rules looking for DLL hijacking candidates in ZIP/RAR archives

Hijacking DLLs in Windows

TL;DR *– DLL Hijacking is a popular technique for executing malicious payloads. This post lists nearly 300 executables vulnerable to relative path DLL Hijacking on Windows 10 (1909), and shows how with a few lines of VBScript some of the DLL hijacks can be executed with elevated privileges, bypassing UAC.*

Reference: *https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows*

Further research: Signed xStart - Elysion

- There are a couple of digitally signed samples of xStart:

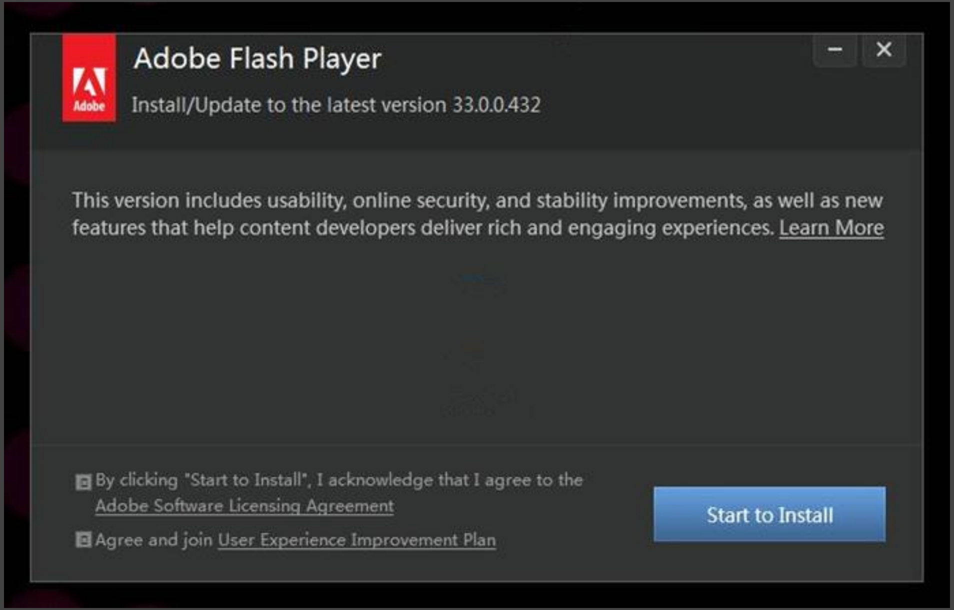
SHA256	f9becebb6c9731732d4f5fa04e2946b9f9cdf20f9d15527b549ffffd0e818775
Compilation timestamp	2020-11-04 02:50:23
Signed by	주식회사 엘리시온랩
Translated	Elysion Lab Co., Ltd.
Serial	03 D4 33 FD C2 46 9E 9F D8 78 C8 0B C0 54 51 47

Further research: Signed xStart - Eagle Investments

SHA256	e385d780f22dbda199c0fe7b778d9d7be76c9ced426fbaf81bc9594c4748bc8f
Compilation timestamp	2020-09-15 08:49:05
Signed by	Eagle Investment Systems LLC
Serial	61 6A AE 89 22 BB 78 E2 16 0A 73 05 61 06 B7 BB

Further research: More signed samples

- Over 60 samples found that are signed with the Elysion or Eagle Investments signing certificate
- Many are tagged by AV as Cobalt Strike/Meterpreter binaries
- Some fake flash player installers
- More Alibaba spoofing, e.g. ‘`aliyun-sec[.]cf`’



Adobe Flash Player

Install/Update to the latest version 33.0.0.432

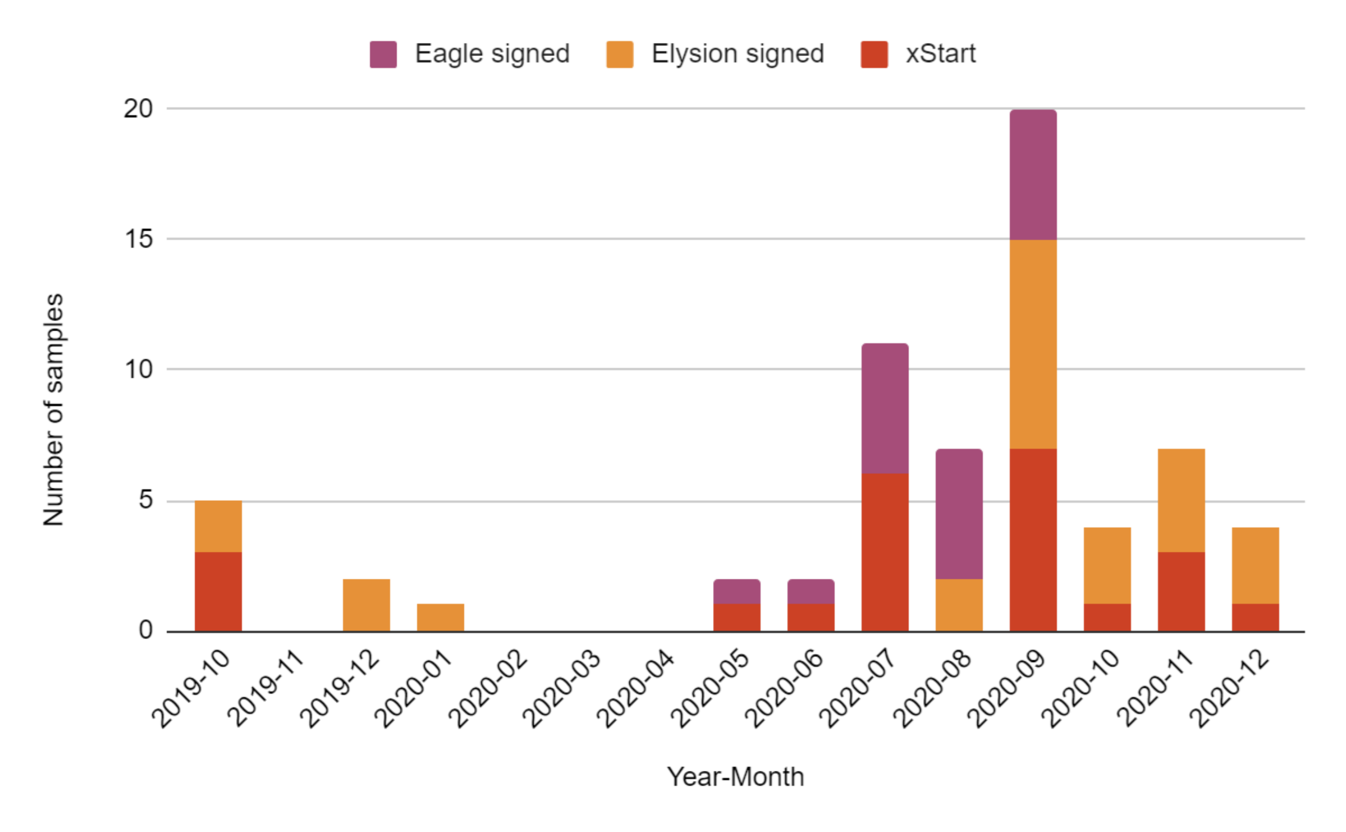
This version includes usability, online security, and stability improvements, as well as new features that help content developers deliver rich and engaging experiences. Learn More

☑ By clicking "Start to Install", I acknowledge that I agree to the Adobe Software Licensing Agreement

☑ Agree and join User Experience Improvement Plan

Example:
`02efd5f4d8dedabeab8e75f3e49a8fdb05c28dfd39bc1e5c96e8213fe3212e9f`

xStart vs. Elysion + Eagle signed binary timestamps



xStart decoy documents summary

SHA256 of xStart dropper	Lure Theme	Likely target sector(s)
b64a4cd485f72e9ce1503b50cd2b5f9f0d8e08d7616543e4acfa559a9b05af34	Titled “Securities Fund Settlement Application Form”.	Financial Services
e7357b82378dd30074b15b69f6b729c29d4d0b666a345e4739e8d6414ab47fe5	Titled “Overlord clauses exist in the student loans of Nanjing Bank of China Nanjing Chemical Industry Park Sub-branch”, which is a letter from graduate student about a loan they took out.	Financial services
204458beb4f170ec21b8ab0bf45987c83c0f4a717e743e698b211c124e480d69	Titled “Feedback from Xi'an Bank Oracle Software Product Maintenance Service Bidding” - looks like an invitation to bid for a project.	Financial Services, Technology
2170b8b11425b62cdc0bc1df85664130961cca921a70dc2ec6da088e04ce59c1	Titled “CDB Windows System | Information Security Deployment Specifications” – “CDB” likely stands for “China Development Bank”.	Financial Services, Technology

xStart decoy documents summary

SHA256 of xStart dropper	Lure Theme	Likely target sector(s)
0bff0d4bcbd5545072b5f8f87d0982cbcdfc66021a2bad486fa2111bf68be60d	Appears to be a complaint form from an employee – mentions "Three Gorges Information System Development Project".	Energy, Utilities
4464be687305f8b23be470b4167c1d9eda39c1dac9d19fa3e2e89d78491c3a15	Titled “China Datang Group Solar Energy Industry Co., Ltd. 2020 Special plan for network information and public opinion security during the national "National Day" period”.	Energy, Utilities
f38b65df5a1ec605c189e6b586455ff444b48a69b3f13bb62550e9e57852cf05	A job application for “Wang Wei”, provides an address of the Shanghai People's Government building.	Government, Political
8f0b2fa58681e92c0f0a37b289de6c6c92a309f93ba89dfad9591b7176fb0b44	Titled “Life Property Insurance Staff Recruitment Application Form”, with details filled in.	Insurance

xStart decoy documents summary

SHA256 of xStart dropper	Lure Theme	Likely target sector(s)
7cf35f3608bfd16f83a315ad413354dc49ffc31668ab87e7bcda6389b1211dc5	Describing a “building sweep” of Kuaishou (a software company that develops a popular video sharing app popular in China) for the visit of the celebrity “Yang Mi”.	Technology
f3f03ad36422f4eb64f6ed05d3bfc83bc8d8ef170e9000d82ab9834e7f469a36	Has the title “About uninstalling the illegal collection of personal privacy apps”, which contains a list of apps that need to be uninstalled by Government order.	N/A
00aa72cf0eedcdcdf48b582160da255c260525f347e2af5cb23a0c328586a2dc	“Proposed promotion list” with empty fields to be filled in.	N/A

MITRE ATT&CK References

Phishing: Spearphishing Attachment - https://attack.mitre.org/techniques/T1566/001/
User Execution: Malicious File - https://attack.mitre.org/techniques/T1204/002/
Abuse Elevation Control Mechanism: Bypass User Access Control - https://attack.mitre.org/techniques/T1548/002/
Access Token Manipulation - https://attack.mitre.org/techniques/T1134/
Hijack Execution Flow: DLL Search Order Hijacking - https://attack.mitre.org/techniques/T1574/001/
Subvert Trust Controls: Code Signing - https://attack.mitre.org/techniques/T1553/002/
Process Injection - https://attack.mitre.org/techniques/T1055/
Indicator Removal on Host: Timestomp - https://attack.mitre.org/techniques/T1070/006/
Deobfuscate/Decode Files or Information - https://attack.mitre.org/techniques/T1140/
Hide Artifacts: Hidden Files and Directories - https://attack.mitre.org/techniques/T1564/001/
Masquerading: Match Legitimate Name or Location - https://attack.mitre.org/techniques/T1036/005/
Obfuscated Files or Information - https://attack.mitre.org/techniques/T1027/
Application Layer Protocol: Web Protocols - https://attack.mitre.org/techniques/T1071/001/
Application Layer Protocol: DNS - https://attack.mitre.org/techniques/T1071/004/

References

Threat Intelligence Reporting:

‘Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organisations’, Recorded Future, *https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf* (28th July 2020)

‘Threat actor leverages coin miner techniques to stay under the radar – here’s how to spot them’, Microsoft, *https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/* (30th November 2020)

‘Hijacking DLLs in Windows’, Wietze Beukema, https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows (22nd June 2020)

Python Scripting:

PyCryptodome - *https://pycryptodome.readthedocs.io/en/latest/src/introduction.html*

pefile - https://github.com/erocarrera/pefile

Python 2 CryptDeriveKey - *https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/flareon2016/challenge2-solution.pdf*

Indicators + Yara rules + scripts:

https://github.com/PwCUK-CTO/SANSCTISummit2021-xStart

Thank you

pwc.co.uk/cybersecurity

🐦 @BitsOfBinary

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.